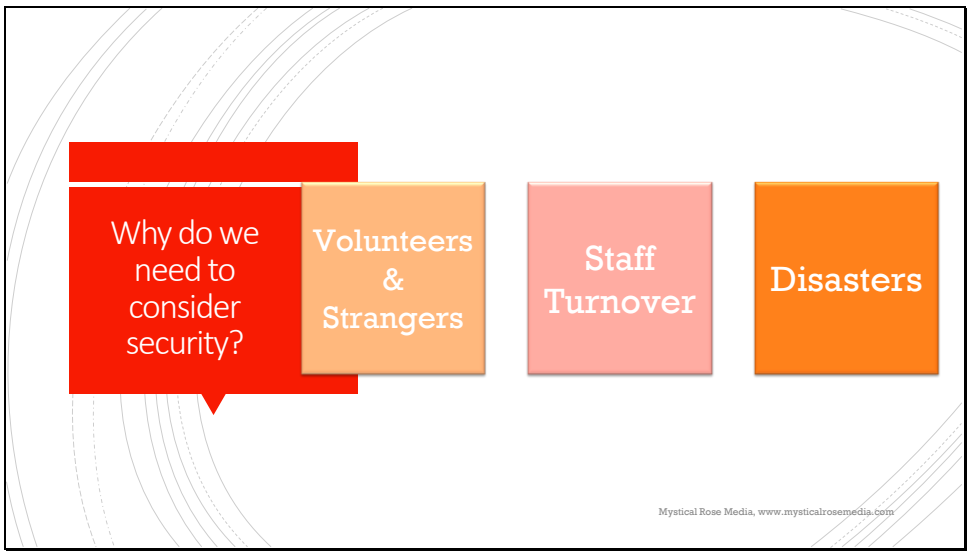
Slide 1


Physical and Digital Security
Things to Consider for your Non-Profit
Mystical Rose Media, www.mysticalrosemedia.com

Slide 2

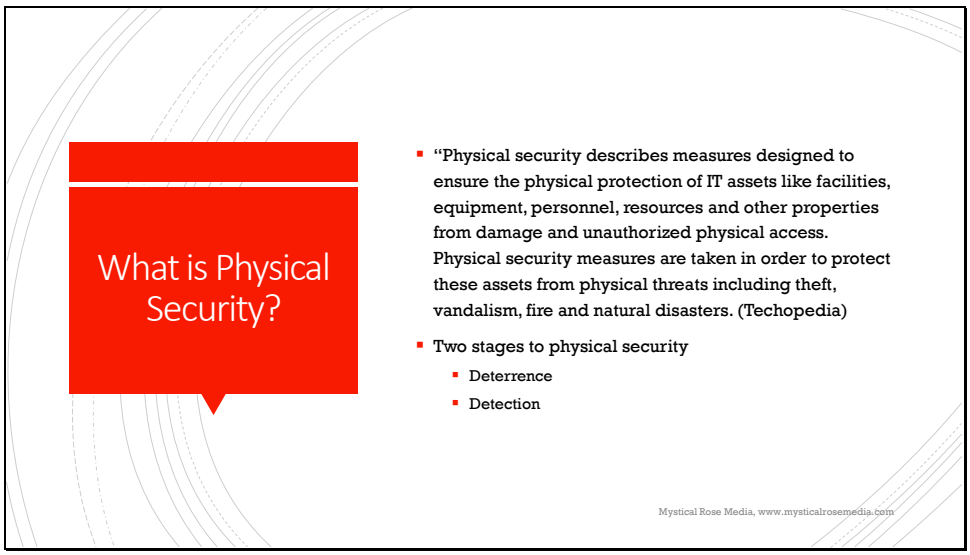


As non-profits, you rely heavily on volunteers to help. This is not always a good things. Allowing a complete stranger into your studios, without knowing exactly who they are, gives them access to areas and equipment they should not have access too. By implementing security measures, we decrease the chances of harm done to the station. Volunteers may purposefully or accidentally bring harm to a station.

This also applies to staff members who are let go or leave. There may be animosity upon departure that may tempt a person leaving to download viruses, steal equipment, change passwords, disconnect cords.

Natural disasters come in forms of tornados, hurricanes, floods, power outages. Any natural event that may cause damage to transmitters and studio sites. Disasters are not only natural, you need to consider safety, terrorist attacks and work place tragedies.

Slide 3



Deterrence is Methods and measures that are meant to deter attackers and intruders or prevent natural events and accidents from affecting protected assets. The simple method for this is through the use of physical barriers and signs. The signs serve as a warning to any intruder that their actions will bring physical harm or prosecution. The physical barriers are meant to prevent access entirely or simply to provide protection from external factors like storms or vehicular accidents.

Detection Allows personnel to detect and locate potential intruders using surveillance equipment like cameras, motion sensors, security lights

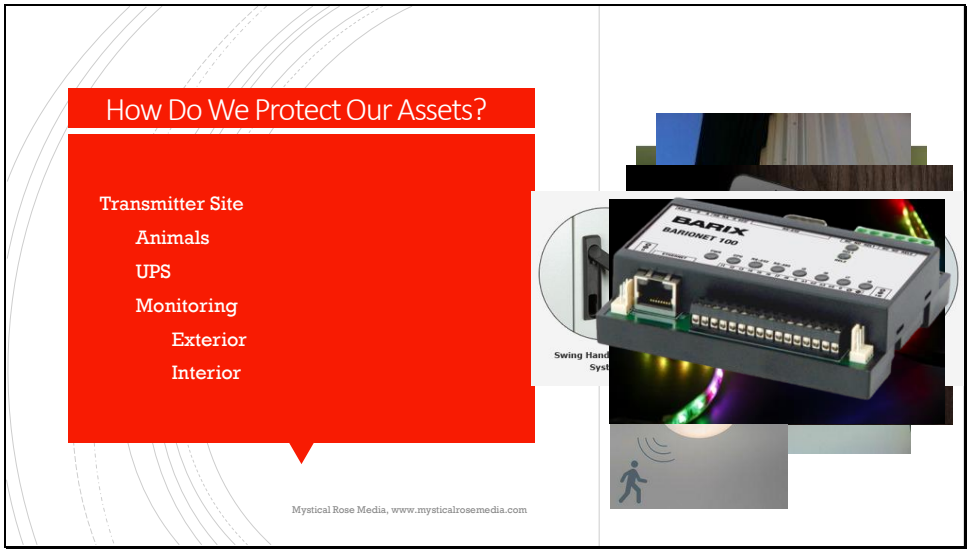
Slide 4

Determine your security risks. Who's got keys and passes? Are the key cards or locks changed when employees leave the company? Are there security cameras (with someone monitoring them) posted in your parking lot, garage, lobby and hallways? How do people exit the building and when they do, where should they go and who should they contact to let everyone know they are safe?

What deciding which security devices and means to go with, the first thing is to plan. What are our most important assets? Secondary assets? How are we protecting these most valuable items physically? Can anyone walk into the room and access the on-air machine and Barix boxes? Do we want just anyone having access to these items? Is our studio or transmitter vulnerable to floods? Tornados? Heat waves with blackouts? Are copper thieves a threat?

Answering these questions will be your basis for security. Determine the weaknesses of your site and make a plan to strengthen them, especially your remote sites.

Slide 5



Transmitter sites are typically located in remote areas and can be quite a distance from any type of assistance.

Have you thought about mice? The little rodents that will chew through wires. John Bisset (a writer for RadioWorld) wrote an article on this problem, stating that unmanned transmitter sites were ideal hotels for mice, as the equipment running provide warmth in the winter. He recommends a product called Mice Magic and doing a through crack check at your sites to find possible mouse entry points, and stuff these pockets with copper or steal wool. The article http://www.radioworld.com/columns-and-views/0004/ooooh-that-smell-cant-you-smell-that-smell/340784. He also has a recommendation to keep Bears away, high pressure sodium flood lights.

Uninterruptable Power Source as power backup in case of loss of power. The UPS for the transmitter site is going to be much more heavy duty than the studio site. For example, the APC Symmetra has amazing features that will help keep the transmitter site online in the case of an emergency. It is scalable and rack mounted.

Monitoring the exterior of the transmitter site can be very simple with wireless cameras connecting to the internet already at the site. Security systems have come a long way, they are motioned enabled, app enabled, online, provide two way communication, and they are DIY. Please refer to PCMag.com or other reputable tech review site for the best of 2018. Placement is crucial, make sure you have the best visibility and all entrances covered, if at all possible, secure the camera such that it cannot be stolen easily. Install “Under Video Surveillance” signs

around the fence. You can have the video recording to the cloud, or install a video server at the transmitter site. When the camera is activated an alarm should be sent to the person in charge of security.

Being able to sneak around in the dark allows thieves to work unnoticed. Installing motion sensor lights will deter crooks and allow your cameras to see at night. Make sure they are high enough where they cannot be disabled. Your sensor should trigger only for human-sized objects — not dogs, cats, insects or other small animals.

How secure are your transmitter site locks? Can a determined person cut through easily enough? How about learning to pick a lock on YouTube? How about using keyless entry? A keyless entry can offer guest codes, no keys, weather resistant, long lasting battery. They can also work with the existing internet and an app.

How do we monitor the interior of the transmitter site? Starting by walking into the site, whether they are allowed to be there or not, cameras and lights should be on. Depending on the size of the site, a single camera should be setup to see the entire room. All rack items should be locked. Ideally the rack setup would have a door on the front with a locking mechanism. There are a variety of rack locking systems available. One thing optional here, but advisable, is rack lighting. You can buy a 19 inch rack mounted light, or you can spend a few bucks and get led lights that stick and are flexible. This would help the person at the transmitter site in the case of a power outage. The lights connected to the rack can be battery operated. Also, in general, doesn't hurt to have extra lighting in that area.

If there is a power outage, do you have an alarm system to alert you? If one of the systems goes out, what is letting you know? If the temperature rises inside the site, because the AC unit dies, how do you know? Your transmitter site should have a smart monitoring system that talks to every assets and alerts you when things are not working. An example is the Barionet 100, it's features include Environmental monitoring, logging and alarming and Temperature monitoring, logging and HVAC control, with a web server for control and SNMP capabilities for sending alerts.

Slide 6

Most of the time our studios are easier to walk into than our own homes. We have opened everything up to volunteers and staff members, that don't need access to the equipment. During a pledge drive, we allow many people in who sign up to volunteer and we cannot keep eyes on all of them, and they have access to everything.

Just like at our transmitter, we ought to be monitoring the exterior of the studio with wireless cameras connecting to the internet already at the site. We should have a security system that is always on during the work period, and motion sensored after hours, app enabled, online, provide two way communication, and DIY. Placement is crucial, make sure you have the best visibility and all entrances covered, if at all possible, secure the camera such that it cannot be stolen easily. Install "Under Video Surveillance" signs. You can have the video recording to the cloud, or install a video server at the studio. When the camera is activated after hours an alarm should be sent to the person in charge of security.

Again, like at the transmitter, lights are important. Again, motion sensored in areas that are not widely used, like the server closet/room. Installing motion sensor lights will deter crooks and allow your cameras to see . Your sensor should trigger only for human-sized objects — not dogs, cats, insects or other small animals. The lights should be on the outside of your building as well, allowing for cameras to do their jobs.

How secure are your studio locks? Can a determined person break through easily enough? How about learning to pick a lock on YouTube? Here a keyless entry system would also be beneficial.

Ideally the rack setup would have a door on the front with a locking mechanism. There are a variety of rack locking systems available. One thing optional here, but advisable, is rack lighting. You can buy a 19 inch rack mounted light, or you can spend a few bucks and get led lights that stick and are flexible.

The biggest thing to remember with layered security is Deny by Default and Need to Access policies. If a person comes into the studio once a week to record spots, they do not need access to anything else in the studio. They should be allowed entry to the productions area and those assets. By default, volunteers and staff do not have access to anything unrelated to their role.

Your on-air machine with the Barix boxes and everything related can be placed in a rack setup, server closet/room, that is restricted to only those who need access, your programmer, audio engineer, engineer. Your on-air machine and Barix units are priority assets, equal to your internet modem/router/switch. This too should be placed in an off-limits area. This should only be available to your IT person. If you have backups kept on site, they should be placed with the modem/router/switch. Don't overlook the fact that some workers may back up their work on USB keys or external hard disks. If this practice is allowed, be sure to have policies in place detailing what is allowed to be stored. If you don't want employees copying company information to removable media, you can disable or remove floppy drives, USB ports, and other means of connecting external drives. Simply disconnecting the cables may not deter technically savvy workers.

Opt for rack options when possible. By using a rack system you can easily place all your priority assets in one unit, locked. Rack units can also be bolted to the floor for further deterrence.

Workstations are vulnerable, especially the receptionist’s at the front of the office. Additionally, you may have workstations that are unused, for temp work, pledge drives, or an employee who is vacationing. This workstations need to be secured. Disconnect and/or remove computers that aren't being used and/or lock the doors of empty offices. We will talk about digital security, but you can think about the possibilities of locking down computers that are available in the open with biometric readers or smart card readers. Many laptops nowadays have biometric readers.

Workstations that have a case are easy to open and grab the hard drive. You might have an accounting computer, customer information, sensitive information on your machines, or your entire stations audio library. Consider putting locks on the cases to prevent opening.

If your employees work on laptops and there is sensitive information, you can invest in laptops locks, such as Combo Lock.

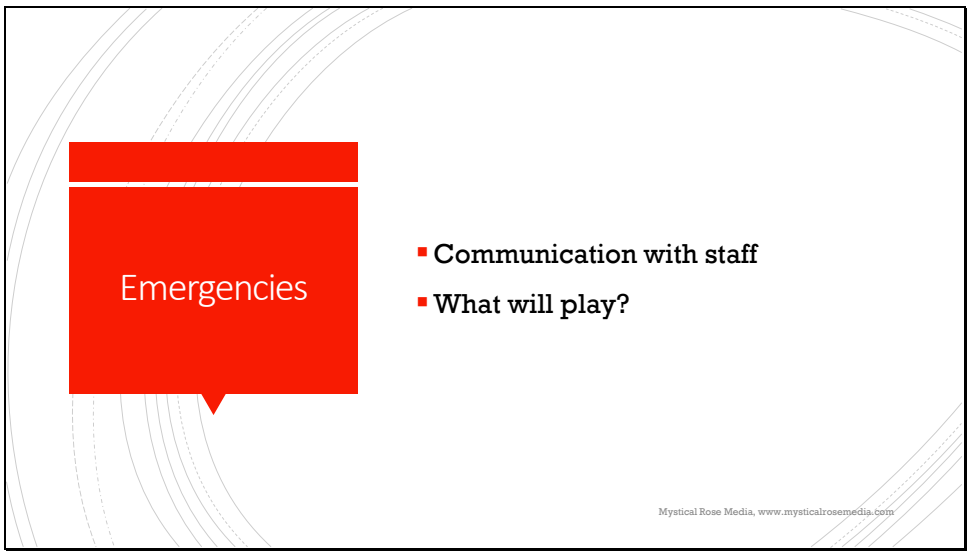
You might not think about printers posing a security risk, but many of today's printers store document contents in their own on-board memories. If someone steals the printer and accesses that memory, they may be able to make copies of recently printed documents. Printers, like servers and workstations that store important information, should be located in secure locations and bolted down so nobody can walk off with them.

Also think about the physical security of documents that workers print out, especially extra copies or copies that don't print perfectly and may be just abandoned at the printer or thrown intact into the trash can where they can be retrieved. It's best to implement a policy of immediately shredding any unwanted printed documents, even those that don't contain confidential information. This establishes a habit and frees the end user of the responsibility for determining whether a document should be shredded.

Visiting a site like http://securtech.com/computer_locks.htm will provide examples of the different types of locks.

Just like before, all of this is not worth it if there is no alarm to sound when something is violated. Cameras, security system, locks should all send an alarm, via app, SMS, or email.

Slide 7



Are you prepared to communicate with your staff in the event of natural disasters, terrorist attacks, or workplace tragedies?

Smartphones have made it easy to create a group message that will allow you to communicate dangers. For instance, the military employs a mass message system when emergencies arise making sure all know the situation. The emergencies are everything from active shooter to roads being to dangerous to drive. Setup the group in advance making sure all mobile numbers are correct. More than one person should be in charge of communicating emergency information. Does your staff know who to call after they've called 911?

Evacuation routes, from the building, should be posted and distributed.

What will play on the air if the station has to be evacuated? Most of the stations are automated, is the station ready for an emergency?

Slide 8


Digital Security
Hackers are everywhere. They get close physically and digitally, and can infiltrate silently. Hackers are not necessarily malicious code geniuses, a hacker is anyone who uses a computer to gain unauthorized access to data. A hacker could be anyone, come from anywhere, and have any reason to steal data or destroy assets.
Mystical Rose Media, www.mysticalrosemedia.com

Slide 9

The biggest threat to digital security is the internet. Like it or not, the internet is where we live, everything is connected. Our Barix boxes need the internet to play EWTN and we use internet to send the feed to the transmitter and so no. Disconnecting everything is the wrong approach, securing it is the way to go.

Manx Technology Group Limited in May 2017 stated according to the Verizon Data Breach Incident Report, data breaches were more common in small than large organizations (25% vs. 20%, with 50% from size unknown) because they lacked the security capabilities. This emphasises the need for a small business to use a firewall to defend their business. https://www.mtg.im/the-best-firewall-router-for-a-small-business/

Slide 10

Passwords seem to be the most basic item, but it is also one of the most important. Default passwords on systems are easily found online and in the manuals. Change your default username and passwords, this includes your EAS system and modems.

Your staff should be required to pick a difficult to break password, A strong password must be at least 8 characters long. It should not contain any of your personal information—specifically your real name, user name, or even your company name. It must be very unique from your previously used passwords. It should not contain any word spelled completely. It should contain characters from the four primary categories, including: uppercase letters, lowercase letters, numbers, and characters.

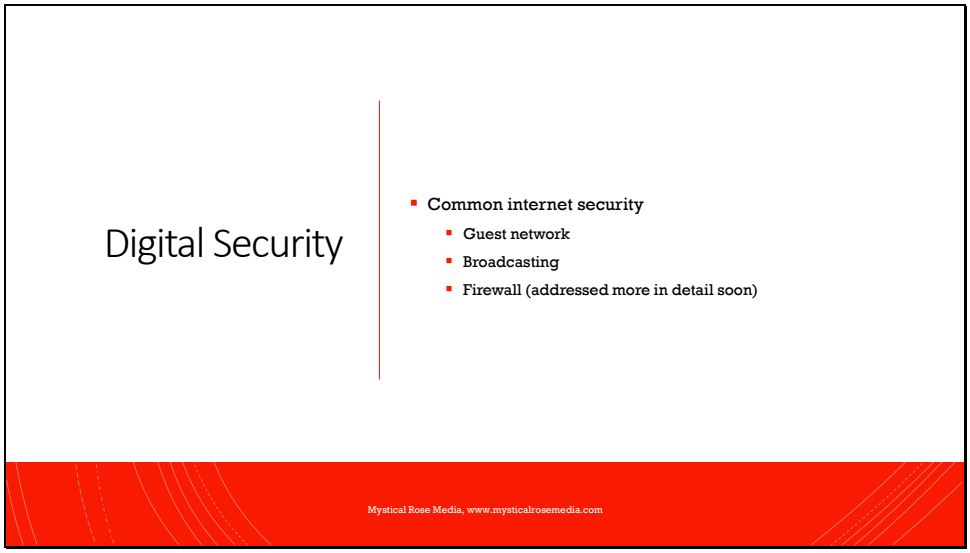
Storing passwords is also important. Using LastPass is a good idea. It will help you remember these passwords, and you can secure your passwords with a master password.

On the computers, remove all programs that are not necessary, and disable all services and features that are not needed. Close all ports that are not needed, keep your OS updated, disable Telnet, an unsecured, old, method of communication

Use a firewall, but not a firewall alone. Deny everything. Open only needed ports. Implement Access Control List (ACL). Keep in mind that a firewall adds latency, and this can affect real time broadcasting. Invest in a firewall with the appropriate processing time.

Your overall health of your computers can be compromised by the tiniest infraction on the part of a volunteer. I once had an on air computer that was riddled with viruses, because a volunteers kid was left alone and he found an unlocked, accessible, computer and started opening everything, exploring, and unintentionally hindering on air play.

Slide 11

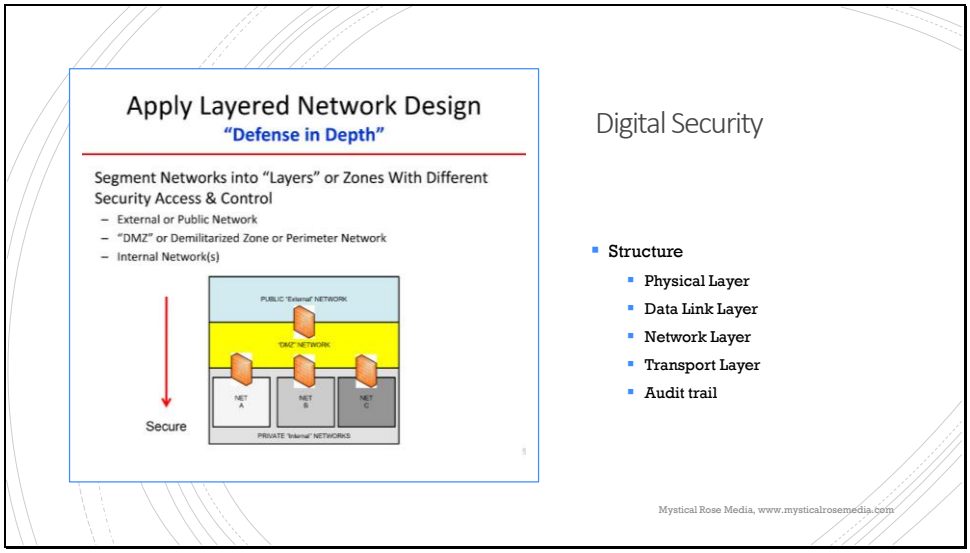


You may have the need or request for volunteers and others to access the internet on your network. This should be a separate system from your main internet running the rest of your network. It is advisable to setup a guest network for them to connect to that is very limited in access to other systems. When you have to computers on the same network, they can see each other, and therefore, they can connect to each other. My allowing outsiders to connect to your main system, you have opened up the opportunity for them to reach all the connected systems, including your audio library, production, and air machines.

Broadcasting is another thing that can be turned off. Instead of advertising your internets name, it is kept hidden from roving bandwidth hackers and malicious persons.

Which one? Are they not the same? The truth is most routers have firewall functionality, and firewalls have router functionality. Although, a firewall will have more advanced features than your combo unit. There are solutions for this.

Slide 12



Your security structure should start at the physical layer, this includes locks on racks and so on, as previously discussed.

The data link layer is the basic connectivity layer. Implement a managed Ethernet switch with security provisions. You can control what can be connected to the network by utilizing switch port security. Configure switch to shut-down port when a violation occurs. Implement segmented or separate network traffic into different domains. This approach also can improve network performance by limiting a network broadcast.

At the Network layer implement firewall filtering techniques and encryption between critical network devices. Firewall techniques included Access Control Lists and/or the network border. ACLs Access Control Lists (ACLs) means all network traffic incoming or outgoing needs approval. This method does take some commitment, but it ends up being very secure. Implement Ingress and Egress filtering. Egress is restricting your internal users from getting off of your network and going anywhere they would like. Ingress filtering verifies incoming traffic is from where it says it is from. Deny by default. Do not overlook internal firewalls.

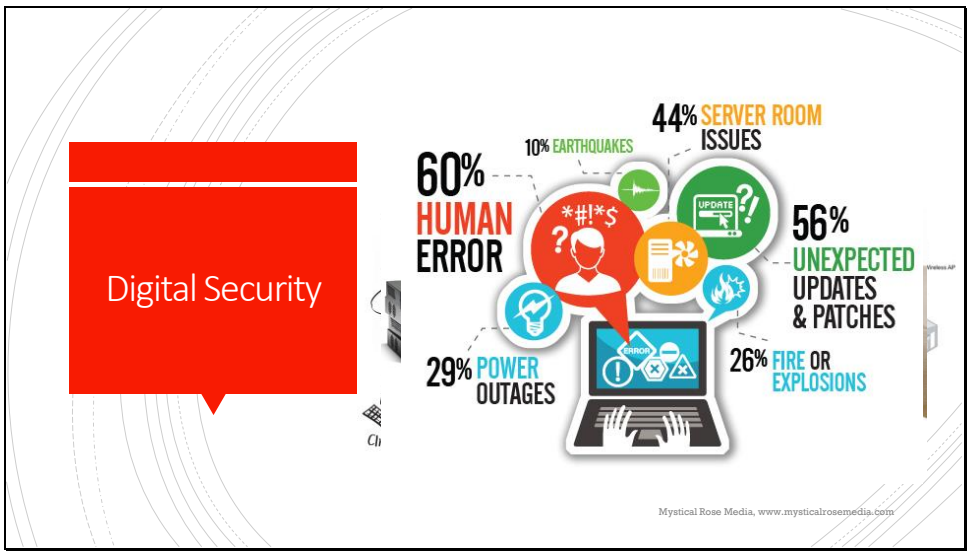
The Transport layer provides another opportunity to implement encryption, includes techniques such as Secure Sockets Layer (SSL).

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 give indication of potential threats being imposed on the network.

The image is an overview of Defense in Depth, network security.

Slide 13



There is a good chance your setup will look complicated, there is a device called a UTM, or unified technology management device. The image is provided by Forinet, which has very good ratings for firewall and business security applications. They are a provider of a UTM device that consolidates you security devices and needs. For easy management of your small business, this is an investment, but would be worthwhile to look in to and price out between different companies.

Most likely, you will need to raise the money for a UTM system, so we will discuss your SMB network. When designing your network, with security in mind, ask what are your primary needs. Do you have staff? Do you need wireless connections? Will wired suffice? If you need wifi, who do you need it for? Will a guest network only suffice? How will you segment the office? Does the accountant or office manager need access to the on-air machine? Production machine? Which computers need to talk? Which persons need access to which computers?

Most likely a hybrid mode will work, a mix between wired and wireless.

We start with the modem. While there is a good chance your ISP will have business modem options, you may want to do your own research before agreeing to use theirs. Sometimes it is required.

Your firewall is going to be a piece of hardware. You have Fortinet, Cisco, Barracuda. Many options to chose from. Research and review. When should you opt for the software firewall solution? While virtual software-based firewalls are great at protecting individual users, they

become costly and over-complicated when several users are trying to operate on one network. In this case, a hardware solution is better suited to the job. A single firewall appliance extends protection to all users on a network. If your organization consists of just a few users, software firewalls could be a workable option. However, if your organization is made up of more than 3 or 4 users, a hardware appliance is an obvious improvement over their software counterparts. https://www.firewalls.com/blog/best-small-business-firewalls/

If you are overwhelmed by the entire firewall decision, talk to an IT service that offers these managed services for you. I have a friend that runs these services on discount for Non-profits and specializes in Fortinet.

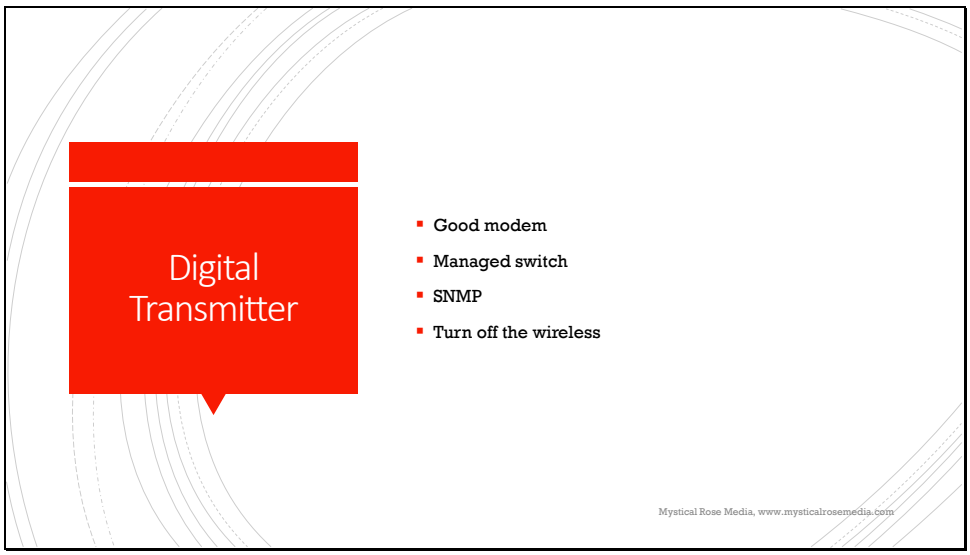
The managed switch, especially at the transmitter, we use for prioritization. An example is the Cisco 300 series, it has IPV6 capabilities, prioritization (AKA QOS), and a web interface for configuration.

The router - Something like the ASUS shown can be close to $300, but the features and speed are amazing. It will allow you to connect a NAS device if necessary. Honestly, spending less than $150 is not going to buy you a good router. You can connect wifi and wired devices. You can also us this extension to segment your network between basic office computers and the guest network and your more critical machines, on-air, production, accounting, and so on.

You can also manage your network more in depth with a server and a NAS device.

Don’t forget disaster recovery once you are setup. UPS sources and cloud backup are mission critical.

Slide 14



The chances are your transmitter site is remote and rarely visited. There is also a good chance everything in your transmitter site it internet capable and has an ethernet port. Having an upgraded modem is going to be helpful. There are many things you can do with an upgraded modem, remote access, priority ports, see if you all your system are connected.

You will also want to invest in a managed ethernet switch (NOT unmanaged), this will also help with prioritizing internet traffic and systems. Some may have their whole setup at the transmitter site, or an STL connection between two sites. You will want these assets to have first shot at bandwidth, this helps with real-time devices that suffer due to latency. They also feature the ability to configure, manage, and monitor your network.

Managed switches use Simple Network Management Protocol, SNMP, for monitoring devices on the network, SNMP allows you to remotely monitor the network devices, so you don't have to go to the site to make changes or troubleshoot the switch.

Why should we care about SNMP? Modern transmitters use this protocol for communication.

http://ireasoning.com/mibbrowser.shtml

This being said, there is no reason for wifi to be available outside the room or to be broadcasting. All your equipment will come with ethernet ports, by using a switch and a upgraded modem, everything will be self contained within your site. If you need wifi up there when you get there, bring a laptop, or have an app enabled modem, turn off the broadcasting,

setup a secured wifi password or guest network. Just because we are used to wifi, doesn’t mean it always has to be on. Some routers allow you to time wifi, if you know you are going to be there at a certain use remote control and set the time, in case you forget to turn it off when you leave.

Slide 15

The last step in security is monitoring and updating. There is no point in running UPS systems if you do not check if the batteries are operational. There is no point in security measures if they are not tested, monitored, and updated as necessary.