Foreign Network Workspace: Overview and Considerations

East Carolina University

Ryan Daley

Abstract

In the ever growing and increasingly intertwined world of networking, as an IT manager / CIO, you may come across the need to create a "local" workspace within the confines of a foreign network. When planning the deployment of a workspace that's location is within another companies network and physically located within the confines of a building that is managed by another governing corporation. Developing a new site can be a complicated and hazy area of planning, policy and risk management, however when considering the site is meshing two governing bodies, it can drastically increase the complication. Currently, my company (a radiology firm) is developing an offsite workspace for our employees within a remote hospital that is not under our management. The research shown in this paper is a baseline for a remote integration, post trial and error of a real-world production integration, highlighting the planning, risk evaluation, and policy development as referenced and compared with existing literature on the previously mentioned topics.

Keywords: Information Technology Management, Risk Analysis, IT Policy, Project Planning

Contents

Overview

I work as a system administrator / PACS administrator for a radiology firm on the east coast of North Carolina. As a company, we employ over 50 radiologists. These radiologists are divided into two sections, on-site and off-site. Essentially, we have our own medical imaging locations that tailor towards patients that are referrals from smaller practices and have services such as; magnetic resonance imaging, computed tomography, ultrasounds, fluoroscopy, mammography, etc. These medical scans are done on-site, and read on-site as well as the patient gets to see the radiologists and speak with the them in person, real time concerning the results or whatever other questions they may have. However; the other half of the radiologists are essentially "rented" to surrounding hospitals. This is extremely common practice among radiology. Hospitals will pay to have a company's radiologists on-site so they can interact with patients as well as consult with other doctors in person to compare findings to diagnose patients more accurately, once again in real-time. We find, as well as the hospitals that rent our radiologists, that even though a patient never technically has to "see" their radiologist to get effective treatment, the face to face interaction and free flow of questions increases patient satisfaction. Due to the increase of patient satisfaction it is becoming more common practice in a sort of reverse technology fashion, seeming to shift away from the more advanced option of remote reading. The technology is present to have entirely virtual remote radiology reads, however it drastically decreases patient satisfaction, in turn hindering business over increasing it. As a company, we rent roughly 25 radiologists to a surrounding 12 hospitals. For larger hospitals, we will have two on site, for smaller ones we will only have a single, and they will often rotate shifts covering hours 24/7/365. Moving radiologists on-site to another location's "foreign" network lends to a very broad, and unique set of challenges to medical IT and even more specifically radiology IT. This research

paper documents the methodology of the integration, compares the process to existing literature, as well giving a bird's eye view of the integration of a 13th hospital into our network.

Audit of Foreign Network

When integrating two networks it's paramount to audit the preexisting structure you are planning on meshing with. This is to insure that the network meets your standards and security requirements, and to highlight areas that aren't quite up to par. Basically, this security audit would be like anything they would pay a third party to do. There are three main areas to auditing any company in terms of security that need to be addressed, these are: An audit of existing policy, operational security standards, as well as IT security standards. Traditionally in IT, we are accustomed to merely the IT security audit section, however when it comes to total security posture, it is much more multifaceted than that. Granted, this isn't "your" network, but since you are essentially entrusting your data to potentially pass through this network, it is extremely important that you find points of improvement, as these weak points if undiscovered and unaddressed could potentially become a weak link in your own network.

Audit of Policy

During the policy audit, you want to see if there are any pitfalls in the way the business runs, not necessarily in terms of IT directly, but in terms of how the companies' employees interact with IT. Policy is generally broken down in to a few major categories:

- **Policies regarding general users:** These are policies that govern things that directly affect end users. Regulations like password length requirements, if passwords are on post-it notes, password expiry regimens, as well as PC idle to unlock time frames, if each

user has their own log on credentials, and other critical items like BYOD provisions (SANS Institute , 2003). This area also governs things that wouldn't directly impact a third party business much less like how they back up their work related data, Physical security of the data (i.e. don't rest your drink on top of your desktop), etc. When auditing these types of policies, which are often the hardest to change due to the amount of people it would affect, it's very important to be concise and specific on what could potentially affect your network and how (Netaji Subhas Institute of Technology).

- **Departmental Policies:** Policies that fall into the department level are things along the lines of chain or hierarchy, for example: documentation on exactly who is responsible for what issues. A real world example of departmental policy in action would be, for example, we are having a connection issue between that hospital and our main location, we have determined that the problem is not on our end, who is responsible for the downtime? Also included in departmental policy would be things like; defined procedures in the case of fire, natural disaster, physical intruder, as well as an intercom based alert code system (i.e. code green could mean a suspicious subject is onsite). These are all things that could potentially have an effect on your assets that are located on foreign ground. These assets being workstations, servers, or even radiologists. You want to make sure the departmental procedures are locked down, as well as making sure the employees you are sending to the remote site are up to speed on these policies (Greenland, 2008).
- **IT based policy:** Auditing IT policy is also important, as these people are statistically more likely to be the ones to compromise the network. To prevent this, it's imperative that IT policy is in place that limits the power of each employee as well as outlines what

> they can and can't do in regards to IT infrastructure. Things that need to be noted during an IT policy audit, who owns the data? What department owns each bit of data on the network, it's imperative that there is an internal sense of ownership as well as oversight when it comes to who is responsible for what. Secondly, if a data has an owner, who are the custodians? who exactly is responsible for the administration and maintenance of this data or hardware, this needs to be documented as well as tracked. Once hardware or data has an owner and custodian, is that data limited via. access control policy? or can anyone access this? are their means to detect improper use? When having an external IT force that is wired into your network it's important to evaluate these areas to develop a sense of accountability surrounding with changes or mistakes made within the realm of IT (SANS Institue, 2009).

When auditing these types of policies, it is very important to be concise and specific on what could potentially affect your network and how. Not only to reduce the scope of the audit, but to be respectful of their policies that exist with affecting your network or your asset's integrity or security. Sometimes this lends to a large amount of gray area, which is normal, but with most things (especially IT), better safe than sorry, so pressing issues you believe affect your environment that their administration doesn't agree with can become increasingly important based upon the type of discrepancy. Handling this area with care is imperative, as it often is the area that is most widespread with a much larger radius of impact if a change occurred .

Audit of Operational Security:

The operational security audit is the most straight forward of them all. During this area of the audit the main question you need to ask yourself is "How secure is this physical location?". If

you plan on housing data or assets on site, physical security is not something to be ignored. If someone broke in, would they have legible footage stored, logged, and documented to present to the criminal investigation? (SANS Institute , 2003) What sort of building authentication do they have in place? Do they use the "I know you" authentication? this is a common, and surprisingly effective type of "authentication", that can be effectively employed by companies with less than 50 -60 employees on-site. Basically, since each employee knows the other, an outsider, or potential social engineer would stick out like a sore thumb.

Beyond that, what checks and balances are in place to prevent employees of the company from gaining unauthorized access to restricted areas? what is keeping the front desk clerk from wandering into the wiring closet and bringing down the entire network? Specifically at this location, high profile areas are locked by a traditional key, and other areas simply say "authorized personnel only", which is good enough for some standards, however it doesn't stand up to ours.

There are hundreds of other concerns, such as; Trash disposal services, if a generator is present, alarm system, 24/7 security, are fire extinguishers placed effectively around areas of importance, are there intercom systems, is inventory managed effectively, do water pipes travel over / under the server room, etc (Kabay). These considerations are going to be drastically different for each location, and often a extremely large amount of things should be considered, luckily, M. E. Kabay put together a really effective checklist at http://www.mekabay.com/infosecmgmt/facilities_checklist.pdf

Audit of IT Security Standards:

This is often best left up to experts. Unless you have a specialized security team, there is most likely something important that will get overlooked. Although, something that can be discussed that often contract security auditors don't take into account or consult on is the network structure, data integrity, redundancy, how data flows through the network etc. Security auditors give a report of what your network looks like from the exterior, which is important, however it's still up to the IT staff to work out the kinks within the network architecture. As well as aspects that would affect any on-site data you may have, such as: Can the HVAC handle another server generating heat? are the servers on the ground floor, not risen? Basic concerns that, if overlooked, could potentially jeopardize data (Elliot).

Existing Foreign Network Topology

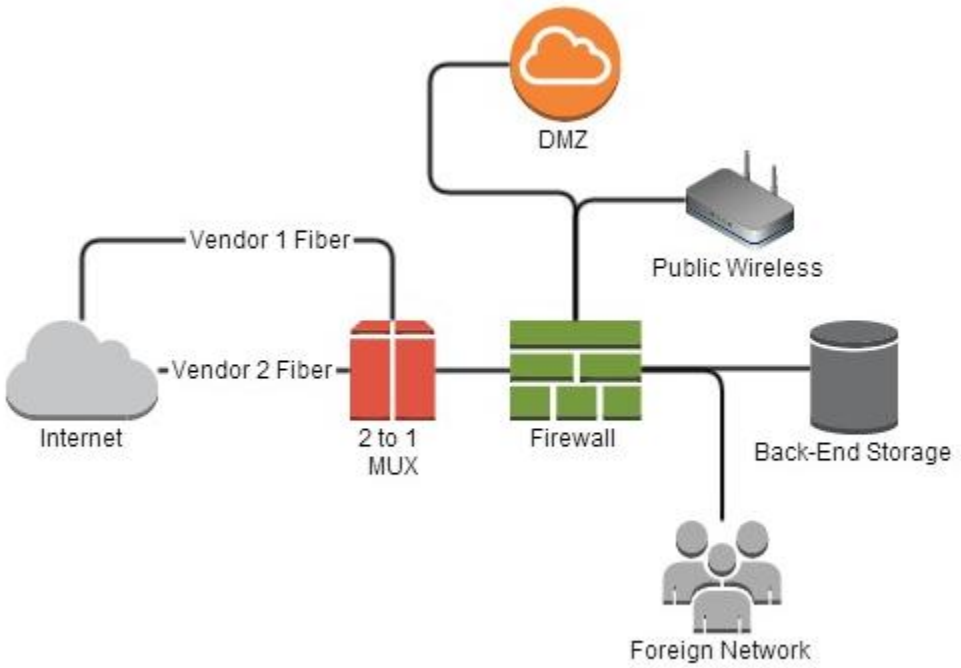

Figure 1.1

Looking above at Figure 1.1, Depicted is a very basic overview of the pre-existing network architecture. There are a few interesting areas of their diagram, as well as a few concerning areas that wouldn't necessarily meet our production standards. Firstly, The method implemented to create redundant WAN connections, is practical, and very "old school". You can see they have two connections coming into a fiber multiplexer, abbreviated MUX. Essentially, a multiplexer allows for a connection to become layered and transmitted over a single signal, ending is a de-multiplexer, where it is decoded back into two connections once more (Ila Gupta, 2012). However, in their implementation, they are utilizing a single multiplexer / de-multiplexer with two WAN connections serving as a form of failover. They aren't load balancing between the two connections, simply if one goes dead, the multiplexer takes input from the other fiber connection. This fail-over is not automated, so when the connection goes down, it is the responsibility of the technician on duty to manually move the connection off the main connection onto the secondary. Beyond the MUX box, you can see they have implemented a single firewall network structure. This firewall delegates traffic between two different private networks, one being their DMZ and patient (read public) wireless, the other being their backend storage and LAN. While a positive in this is that the DMZ is segregated from the "meat" of their network, there are a few downsides. The first downside being that the public wireless is located on the same network as their DMZ allowing for anyone on their wireless the ability to "touch" their DMZ. Lastly, having a single firewall does not allow for the zoning methodology of networking and security. Its imperative that you have a buffer area between the outside world (internet), your servers that touch the outside world (DMZ), and your local machines and your backend data storage (LAN).

Ideally, these three areas would be segregated by two firewalls, creating a buffer between each environment (Ferro, 2009).

Integration

After evaluating what is currently in place at the remote location, we are then tasked with creating a plan that satisfies the needs of each location in terms of security standards. The best way to do this usually, at least in terms of medical, is take action based on who has the "higher" security requirement for the requested topic. Rarely would you hear anyone in charge of IT systems and security say "We prefer the less secure route". With that umbrella mentality in mind, it is also important to consider the security goals of each location to make sure they entire twine closely enough, where the umbrella approach is even relevant. Conveniently, under HIPPA, medical practices have little wiggle room in terms of "Security goals". With all medical practices the top three goals are going to be extremely similar if not identical, making a meshing of networks like this much more simple. The top three most common goals are:1) Patient Health 2) Privacy 3) Data Integrity and longevity (Health and Human Services). Sharing these goals makes it much easier to convince other companies to move on security concerns once presented to them. During this integration planning, there is going to be costs incurred for each party involved, be it facility upgrades, network equipment, training, workflow disruptions, etc. However, since all of these changes relate back to the 3 common goals of healthcare IT, getting funds appropriated towards these goals is much more cut and dry compared to two companies with different goals attempting to mesh. With this in mind, and common goals established we are able to continue planning for the integration.

Integrated Policy

Integrated policy is probably the most complicated of all the aspects associated with combining two networks. The reasoning behind this is because it involves the most change, I say the most change based on the fact that a core aspect of policy and enforcement is companywide enforcement and understanding of the policy and regulations at hand.

One of the more complex, as well as the most paramount security foundations are created on the human level. Considering the IT security paradigm, it's important to realize that security begins in policy, and ends in IT. Business operations and IT security concerns must be meshed to achieve a substantial security posture. There is a direct and substantial correlation between IT governance and everyday aspects of business, and because of this it's important to consider each of these when attempting to align the strategies of the two (Yap May Lin). The difficulty associated with aligning the two areas becomes exponentially more difficult when considering meeting the standards of both entities.

Due to the fact that our workspace will be, ideally, segregated physically from their workspaces satisfies some concerns such as; Shared workstations, users using log on credentials that aren't theirs, un-authorized medical data access, and other concerns of the like are immediately satisfied by a physical separation of workspaces.

On the other hand, there are policies of the location that we have no sway or say so in, perfect example of this would be any type of "green policy" they may have. Since our workspace is going to be attached to their power backbone, and they would be footing the bill, its mandatory for us to abide by whatever standards they may have pertaining to the conservation of power (Elliot). Often, hospitals will pride themselves on we cut this much power causing this much

decrease in carbon emissions, and it's not our place to change this. So what policy they have about machine sleep, monitor powering off when unused, or efficiency requirements on machines (i.e. Energy Star approved) must be considered even if it involves creating a workstation set up to meet these standards.

Another example of gray area that must be addressed, which is different for each integration, is the division of labor associated with on-site repairs or IT support. In my example, this hospital is around 2 hours away from our main IT headquarters, and if something went down on site, given someone was already in the car on the way there, it would take 2 hours to resolve unless some middle ground was developed. Often this middle ground, or division of labor, in terms of IT support is based around the sense of urgency. In our case, we have a policy being drafted that if any outage is business critical, or impacts any of the three goals of healthcare IT, specifically patient health, the remote site IT will be our "eyes and ears" per-se, where we will talk them through repairs if we are unable to do them remotely. Where-as less critical elements, such as a dead monitor or dead mouse, will be replaced on site and billed to us to insure the least downtime. The caveat to this, is that we have to trust their personnel's knowledge and ability, which, given the situation the risk of their IT being incompetent is less threatening than the guaranteed downtime of ~2 hours to fix a problem like rebooting a server etc. Considering this caveat, that is where we would take what we found out about auditing their IT policy and comparing it to ours, to find the best, most secure middle ground. To solve the service issue, we generated a user account that is only a local administrator on the machines located in the foreign network. Not only does this squelch any major concerns about foreign employees potentially reaching or harming our internal network, this also satisfies the HIPPA requirement of "unique

user identification". This is for accountability as well as preventing us giving out our network credentials to a foreign body (Health and Human Services).

These are the major policy discrepancies we ran into, overall the audit showed that many of their training and personnel based policies aligned closely enough with ours, leaving us to simply patch up some gaps between the two.

Integrated Operational Security Standards

In terms of security, the operational gap between our two companies was the largest. Badge based person access was no existent, and the only internal operation safeguards were signs that said "EMPLOYEE'S ONLY BEYOND THIS POINT". This does not meet our security standards, not by a long shot. Our standards dictate that room based badge access is mandatory when entering areas that contain medical data. The purpose of this is to insure who enters and leaves, log it, and save it in case something is found and we need to investigate who was where when. Having a badge forms as a lower level form of two factor authentication, where a badge is something you have, and the password to log into the machine is something you know. Granted, this location had physical key based access to high profile areas like wiring closets and server rooms, however keys don't log entrance and exit data, or increase accountability. They weren't willing to implement building wide keycard based authentication, so we were forced to implement our own, luckily, our key card based authentication was network based, so it was fairly easy to install a key access door into our workspace. Another added benefit to this lends to the basis of the foreign technicians working on our PCs, we distributed access cards that are encoded with a person ID, so if one of our workstations is physically compromised we can see what person entered the room and compare to who logged into the PC at that time, to have a low

level clue on where to being any investigation. Additionally, since the hospital is relatively small, the "I know you" aspect of the area increases the security substantially, granted it's no replacement for access badges, it does work in smaller instances where all the employees are familiar with each other, someone attempting a physical attack on the location would stick out like a sore thumb. Outside of the key based access controls concerns, the location security, i.e. security cameras, footage logging, fire escape as well as other emergency protocols were all up to standard.

Integrated IT Security Standards

This area is more dynamic than the other areas, as most IT security standards are subject to change simply under the discretion of a new vulnerability on the market. Another reason it's so dynamic is because of the simple fact that technology is progressive in nature, so essentially, the integrated standards have to be resilient enough for expansion and growth as well as satisfy the requirements of both parties as time moves on.

After the initial audit, we discovered multiple areas that weren't up to our standards or HIPPA standards. So once again, referring to the 3 common goals of healthcare IT, once discovered the third party was more than willing to allow us to pair with them and essentially put on the hat of a consultancy in assisting them to expand and grow their posture as well as meet some of our standards in the process, allowing our networks to more organically flow together naturally meeting both of our requirements as the network progressed over the development period.

Proposed Finalized Integrated Network Topology

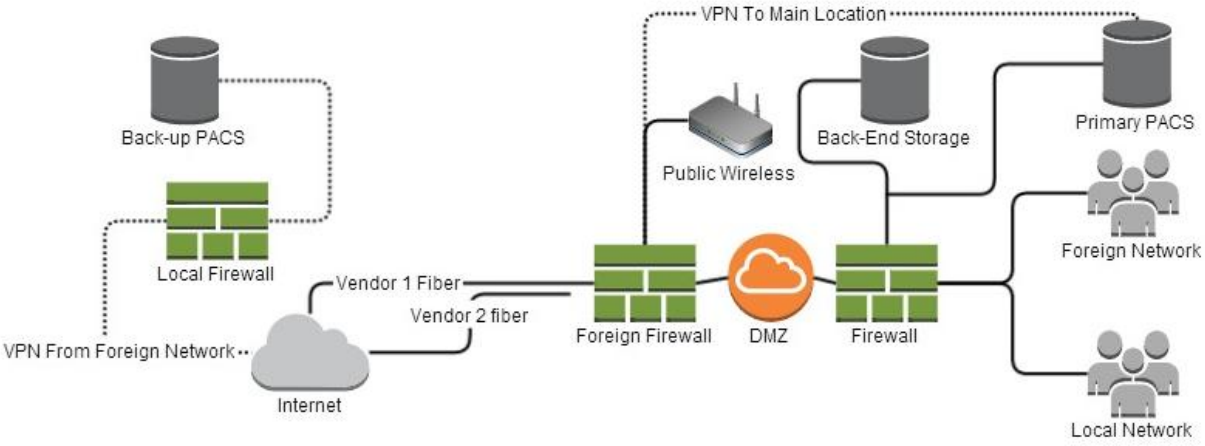

Figure 1.2

Above in Figure 1.2 you can see an overview of our proposed network architecture. Comparing this to Figure 1.1, you can see a large amount of changes. Moving from what many consider a form of "legacy" connection redundancy, the MUX box, to something more relevant and more effective. Currently, many firewalls have the ability to load balance and failover built in, this firewall is slated to be instated as a Cisco ASA. The Cisco ASA firewall has very effective built in protocols for dynamic and seamless failover (Cisco). Another proposed change is creating a network completely separate from anything beyond the first firewall, and essentially treating the patient or public network like the internet, as hostile. Beyond the first firewall, we will place their DMZ, their public facing servers, i.e. imap/smtp servers, web servers, and other items they would like to be available to the internet, but still protected. Insulating your DMZ between two firewalls exponentially increases overall security, where if the first firewall, and a DMZ server were compromised, it wouldn't reach the LAN (Ferro, 2009). The second firewall we plan on implementing is most likely going to be a professionally configured open-source product to off-

set the cost of the ASA. Additionally, just purchasing 2 Cisco firewalls was the plan, however having two identical brand firewalls could potentially open up your entire network if a brand specific bug or vulnerability was to be released. Considering that, it's worth the extra burden of having two different breeds of firewall to maintain.

When it comes to the proposed workspace installation, we decided implement an on-site primary PACS server. After the audit, we deemed their server room to be up to standards, so we piggy-backed on a rack for the primary server. The main benefit of having this on-site is speed. Querying and retrieving medical images can be extremely taxing on a network, so having this onsite would drastically increase the image throughput. The backup server is located offsite, and connected through a VPN that is propagated between both their firewalls, and our on-site firewalls to the offsite backup. As for the actual radiologist workspace, it is placed on their LAN, which will be up to our standards after the network changes occur seen in Figure 1.2 compared to Figure 1.1.

Conclusion

Intertwining networks can be a long and arduous process. A process that involves continuous efforts between both parties. It's extremely important before the process begins to establish common goals, and from those common goals create a baseline to work from, this baseline is created through auditing. Beyond the auditing, compare the findings to your cumulative goals to maintain common ground and work together from there. An integration can be burdensome in the monetary sense, as well as in the sense of policy, operational security changes, as well as IT changes. Meshing two networks is a stout challenge for IT and a company as a whole, however, in the end you receive input from outside sources, and if done correctly, your security posture could be drastically improved when it is all said and done.

Works Cited

Elliot, B. (n.d.). *Auditing a Data Centre - But to What Standard?* Retrieved from bicsi.org: https://www.bicsi.org/uploadedfiles/pdfs/presentations/auditing%20a%20data%20centre.pdf

Ferro, G. (2009). *Designing Enterprise DMZ and multilayer Firewall Clusters*. Retrieved from etherealmind.com: http://etherealmind.com/design-enterprise-dmz-firewall-clusters/

*Greenland, P. C. (2008). Departmental Policy Planning. *Australian Journal of Public Administration* , 369 - 377.

Health and Human Services. (n.d.). *HIPPA Security 101*. Retrieved from hhs.gov: http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/security101.pdf

*Ila Gupta, N. A. (2012). New Design of High Performance 2:1 Multiplexer. *International Journal of Engineering Research and Applications* , 1492-1496.

Kabay, M. E. (n.d.). *Facilities Security Audit Checklist.* Retrieved from mekabay.com: http://www.mekabay.com/infosecmgmt/facilities_checklist.pdf

Netaji Subhas Institute of Technology. (n.d.). *IT Security & Audit Policy*. Retrieved from nsit.ac.in: http://www.nsit.ac.in/pdf/itsa_policy.pdf

*SANS Institue. (2009). Protecting Against Insider Attacks. *SANS Institute Reading Room* .

*SANS Institute . (2003). Security Auditing: A continuous Process. *SANS Institute Reading Room* .

*Yap May Lin, N. H. (n.d.). IT Governance awareness and practices: An insight from malaysian senior management perspective. *Journal of Business Systems, Governance and Ethics* , 43 - 57 .