Chad Ballay

**Week 4**

[Reference Document](https://s3.us-east-1.amazonaws.com/blackboard.learn.xythos.prod/5a31d48b683a8/2035933?response-content-disposition=inline%3B%20filename%2A%3DUTF-8%27%27Week%25204%2520networkdiagram.pdf&response-content-type=application%2Fpdf&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Date=20200411T045202Z&X-Amz-SignedHeaders=host&X-Amz-Expires=21600&X-Amz-Credential=AKIAIL7WQYDOOHAZJGWQ%2F20200411%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Signature=6db42496a9c901a05e3caef762d50e5ab0b15e9b68276db51866c27ae32a6333)

**Identify the relevant information technology (IT) infrastructure domains to envision, design, and develop access controls.**

Workstation Domain

Lan Domain

Lan-to-Wan Domain

System/Application Domain

Wan Domain

User Domain

Remote Access Domain – Not pictured as part of the network diagram but this seems like it would be needed even if to just address the denial of it.

**Develop a basic organization-wide access control plan.**

1. Standup your own or review existing document repository. Define what will be publicly socialized around Access Control Plans and Policy. Depending on the company and culture this will help with buy in.
2. Physical access will be secured as best as possible. (Network closets, after-hours access to facility, IT operations to have a dedicated area, PII/HIPAA/SOX/etc data to be in lockable storage, badged entryways or at least cameras, etc….)
3. Inventory audit of hardware and mapping of physical network. The long term plan would be to know who/what/when/why a change in the IT infrastructure occurs.
4. Hardening the infrastructure. Unused ports in unsecured locations to be disabled. Where able conduits to be used for cabling. Audit and identify the wifi access points and tuning them to not broadcast beyond the physical perimeter as able. Upgrade/Update protocols, firmware, hardware and software as able.
5. Review the current User Account and Access infrastructure. If not already present create an LDAP/Kerberos/Active Directory infrastructure. Define organizational units as well as roles and map these to users.
6. User account auditing and policy enforcement process to be reviewed. Remove administrator access where possible. Remove generic logins and replace with a policy of individual user accounts.
7. Remote access is currently not in scope for this plan so explicitly define how this is enforced currently.
8. Audit existing firewall infrastructure for monitoring gaps. Begin a policy of baselining access and user behavior. Begin by sharing automated attacks/scans prevented. Build a policy of communicating out summary statistics to help ensure the relevance remains on continuing efforts. (This is the easiest of the ones to use to garner support.)

**How would you implement this plan?**

* My first step would be to figure out the core competencies of the business and what is its primary revenue stream. Building a basecamp around using the first and protecting the later. If your company is a fuel distributor you won’t have spare coders laying around. But you will have people who understand safety procedures and physical access controls. Start with what you have and work within that scope first.
* If you aren’t making money for the bottom line then you are an expense so do what you can to be an asset and not a liability. For instance, reach out to identify items that can be done to reduce the insurance premiums and play into physical security of the faculties. Identify when are the key crunch times and ensuring your changes don’t interfere with those times.
* Another key component would be making sure to focus on the long-term plan. Security policy changes impact people and their expectations. Establish the brand of slow methodical improvement. Announce early, proactively explain, and be willing to pause temporarily as policies are implemented. Overzealous, doctrinal enforcement of policy will get your efforts undermined and hampered.
* I would make sure to focus on communication. Security is everyone’s responsibility but everyone else doesn’t have the desire to do the work of security. Their goals aren’t your goals so help them to see the value. Conversation starters about security concepts through prepared light-hearted pranks. Phishing email tests that reward someone for correctly notifying security is the right approach. Not shaming someone to their manager if they fall for the test. Get people aware of the stakes but also engaged in the process.
* Fight the systemic issues at the technological or defined process level and not at the people layer. Lecturing people about external internet access isn’t the right fight. Educating them beforehand that external internet access is monitored, then rolling out a summary recap email each week that shows them their own usage will get you more mileage. The point is that if you don’t fix things at layer 8 of the OCI model.