Building a Technology Partnership to Last

Your Organization's Technology Discovery

Building a Technology Partnership:

The Technology Discovery

For Your Toolkit

Technology Asset Inventory.xlsx

Purpose

As we mentioned in the MSP Getting to Know You Meeting, each company's technology infrastructure is different. Most likely it has evolved over time to meet the changing needs of your organization. There is no one-size-fits-all, right or wrong, technology framework.

This discovery activity is an excellent opportunity to create the big picture of where you are, what works, what could be improved and most importantly, the path that supports your future growth.

If you have network documentation already, that will be valuable for the MSP. However, he will still need to complete his own discovery.

If you don't have your technology documented, then this is the perfect time to create a documentation policy for your organization.

While we focus on the network infrastructure, there is the software application

component that applies to any technology strategic initiative. We'll explore strategy from the software perspective in Discovering Your Software Strategy.

Actions

One or more senior level network engineers will perform this discovery onsite. Often a network discovery tool will be temporarily installed on one of your servers to aid in a complete network evaluation.

This approach is efficient and gathers all of the essential information into documents the engineer can analyze.

Regardless of the method used --- discovery tool or manual inspection --- the engineer will need the administrative password to the network.

While there is no discovery documentation standard, the following are key areas that should be documented.

Building a Technology Partnership:

The Technology Discovery

Network Topology Diagram

☐ 1. Networks change continually so a network diagram from even last week may not be current. Ensure the diagram, if provided, is current.

☐ 2. Includes each network segment, the routers connecting the segments, the servers and all other networking hardware on the segments.

Third-Party Providers

☐ 1. Who provides Internet services?

☐ 2. Who provides phone service?

☐ 3. Are phones VOIP or an in-house phone system? Who provides support?

☐ 4. Are there other service providers?

Servers

☐ 1. For each in-house server, list the server name, its IP address(s), and the role

each server is performing. Each server may have more than one role on the network, and it's important that all of these are documented.

☐ 2. A server may have more than one network interface card (NIC) so each of these should be documented.

☐ 3. Is there a change log for each the server?

Tip: This is an important piece of historical information that an experienced system administrator maintains. If you don't have one now, make sure the MSP recommends that for the future. When problems arise, this is the go-to resource for "what changed and when?" The time and costs to resolve problems can be greatly reduced.

☐ 4. Is any hardware owned by a third party?

☐ 5. Are any servers located offsite? If so, then all of the information documented for in-house servers needs to be documented for these remote servers as well. Who will support these servers?

Other Network Hardware

- ☐ 1. Device name, manufacturer, serial number and age of the equipment.
- ☐ 2. How are these devices connected to the network?
- ☐ 3. How is the device configured?
- ☐ 4. Is there a configuration backup?
- ☐ 5. What version of firmware is being run on each? Is it current, supported or in need of replacement?
- ☐ 6. If there is password protection on any device, who has it, where is it stored and who has access to it?
- ☐ 7. Is any hardware owned by a third party?

Remote Network Access

- ☐ 1. Is remote access supported for employees or third parties?
- ☐ 2. What remote access software is used?

☐ 3. Number of licenses and the expiration dates

☐ 4. Who is the contact for license registration and renewals?

✎ **Tip:** See Housekeeping tip.

Network Software

☐ 1. For each server document the software applications running on it. Include the purpose of each application, the software version, the license number, warranty, support and expiration dates.

✎ **Tip:** Ensuring that valid software licenses exist is important. Unlicensed software is illegal and leaves your organization at risk if a software provider does an audit.

☐ 2. Warranty and support are important to consider. For example, if the software provider will not support the application after a given expiration date, who will provide the support?

☐ 3. Is anti-virus installed and current? Document manufacturer, version, license

keys

☐ 4. How are software updates deployed to the servers? Who is responsible for coordinating updates and notifying all affected staff?

✎ **Tip:** If any servers host production services, these should be noted. Applying updates will require more coordination with in-house staff to minimize service disruptions.

✎ **Tip:** Production servers should not be accessible to all third-party service providers. As you move ahead with this technology partnership, ensure that those technicians with access are senior level support team members.

Active Directory

☐ 1. If Active Directory is used, document the domains.

☐ 2. Document the site structure.

☐ 3. Where do the servers exist within the domains?

☐ 4. Document the groups and content of each group.

- ☐ 5. What external trusts exist?
- ☐ 6. Who is (are) the domain administrator(s)?
- ☐ 7. Are all passwords documented and stored in a secure vault?

Backups

- ☐ 1. How are backups currently being done? What software? When run?
- ☐ 2. What procedures are in place to verify the backups?
- ☐ 3. What recovery and restore procedures are in place?
- ☐ 4. If there is a third party providing backups, who will support the backups if there is a new MSP?
- ☐ 5. Who owns the backup hardware and software?

✎ **Tip:** If backups are being provided by a third-party, it is likely that this provider owns the equipment. Don't take the new MSP's word for it. Contact the current provider and ask how you can preserve your backup if you change

providers.

Desktops and Laptops

- [ ] 1. Document all devices on the network including user assigned to, device name, IP, subnet, manufacturer, purchase date, warranty, serial number, operating system version, last update
- [ ] 2. Are any desktops or laptops owned by third parties?
- [ ] 3. Is any support provided by third parties other than the current MSP?

Client Software

- [ ] 1. Document industry standard software installed on each including primary use, manufacturer, license, version, last update
- [ ] 2. Document proprietary software including primary use, license key, who supports, who owns, last update
- [ ] 3. How are software updates deployed to each PC and laptop?

☐ 4. What anti-virus is installed on each desktop and laptop? How are updates deployed to each device?

BYOD (Bring Your Own Device)

☐ 1. Does the company allow employees to use their own devices on the network? If so, who and which devices?

☐ 2. Is there a documented BYOD policy?

☐ 3. What applications are used on the employee-owned devices?

☐ 4. Who supports the employee-owned devices?

☐ 5. How is anti-virus ensured on each device if applicable?

Housekeeping

☐ 1. Is all equipment clearly labeled with the device name?

✎ **Tip**: Invest in a label maker and attach a device name label to each piece of

equipment.

☐ 2. Are network and phone jacks labeled?

✎ **Tip**: Ditto for the label maker. Label the phone and switch ports on each jack. The amount of time saved chasing cables is well worth it.

☐ 3. Is there are asset inventory maintained?

✎ **Tip**: A spreadsheet works just fine. We've included one to get you started in your Toolkit. Keep it current as assets are purchased and disposed of. Your accountant will thank you when you deliver a current asset inventory each year.

☐ 4. Is secure password storage used?

✎ **Tip**: While we like spreadsheets for a lot of everyday things, we recommend a more secure approach to password storage. All it takes is access by one unauthorized user or disgruntled employee, and the damage can be devastating.

There are a number of free or low-cost password solutions. We have used LastPass happily for quite some time. Give it a try.

☐ 6. Is there a new employee written procedure?

☐ 7. Is there an employee termination written procedure?

☐ 8. Who is the contact for license registration and renewals?

✎ **Tip:** Use a generic email alias such as support@yourcompany.com for all registrations. Include the team members who need to have access to this information on the recipients list. Keeping this list current ensures that important notifications aren't missed.

Thumbs Up

☐ The engineer announces himself on arrival and asks for someone on your staff to take him to the server room.

☐ A discovery tool is used.

- The MSP is committed to collecting as much information as possible efficiently.
- The MSP technical team is more strategic in its approach to service.

- The discovery analysis will be a valuable reference document for ongoing support.

☐ The MSP follows up with an expected delivery date for the report review and proposal. This next meeting should be within 5 business days.

Thumbs Down

☐ No discovery tool is used.

- The MSP does not see the value in a thorough analysis.
- The MSP team does not have the technical depth or analytical skills.
- The MSP has a one size fits all approach. They are more focused on "how many" than on the broader strategic view.

☐ The next meeting is not scheduled within 5 business days.

☐ You have to follow up and ask for the meeting. This is a sure sign to stop here.

Expected Results

The time onsite will depend on the size and complexity of your network. Your MSP will give you a realistic estimate when scheduling the work.

This discovery will not disrupt your business.

Deliverables

Once this information has been collected from your network, the engineers will compile the discovery report. This report will be reviewed internally by the MSP's technical team and the service proposal will be prepared.

What's Next

You will meet with the MSP technical and sales team to review the discovery and services proposal.

Explore the company series --- Building a Technology Partnership to Last

Visit the Quest Technology Group Academy

Let's Connect Anytime

Quest Technology Group
315 E. Robinson Street, Suite 525
Orlando, FL 32801
407-843-6603
www.quest-technology-group.com