What is an IT Assessment?

As different company environments can range from fairly straight-forward and simple to highly complex, we take a look at five key areas. A description of each area included in the assessment is described below:

1. **Security Environment**
   We want to understand what security measures are in place or lacking to protect your business from both internal and external access to unauthorized areas of the IT environment. Here we take a look at areas like physical access to the servers, password policies, admin rights, antivirus, critical updates, SSL certificates, etc.

2. **Network Environment**
   We want to understand your business’s topology. We look at your: LAN—how this office desktops and servers communicate; WAN—how this office communicates with another office and how this office communicates with the Internet; VPN—how remote users (i.e. laptop road warriors) communicate with this office.

3. **Server Environment**
   This is the heart of your computing infrastructure. In addition to the basics (CPU, RAM, OS, disk capacity, etc.), we look for different information depending on the role of the server – domain controller, file & print, Exchange, etc.

4. **Backup Environment**
   This typically falls under the server arena. However, we believe that backups are so vitally important that we break it out separately. We look to see if backups are being performed, the version of the backup software, offsite storage, media, etc.

5. **IT Department**
   We want to understand the business side of your IT department, for example, how you are handling IT support, what type of reporting tools are in place, and what the future goals are for the IT Department.

**Findings**

Our findings are categorized into four severity levels. These severity levels are defined as: Critical—Critical findings are issues that C3 Solutions feels should be addressed immediately to prevent the high likelihood of an interruption of service or loss of data. Important—Important findings are issues that are causing a problem and should be addressed as soon as possible; these issues are affecting performance. Best Practices—Are defined by the vendor to maximize the feature set of the software. Informational—This category is for your information only.

We typically find four or five issues in each category. Sometimes the business was actually aware of most issues prior to the assessment, and sometimes we uncover issues that the internal IT staff was not aware of. Here are just a couple examples of common findings of various severity levels.

1. **Security Environment**
   Critical – The Servers on the network are not up to date with the latest Microsoft Security patches. These patches are critical because they typically resolve security
vulnerabilities which were discovered by exploits. Microsoft WSUS should be implemented to ensure that all computers and servers are updated regularly.

**Critical** – Currently all employees have administrator rights to the entire environment including the servers and server applications.

**Best Practices** – Active Directory is not configured to best practices. There are no GPO policies in place for security and user restriction.

2. **Network Environment**

**Important** – The server is pointing to external DNS in addition to pointing to the internal network. This server should not be pointing to the internet for DNS resolution.

**Best Practices** – Remote access is best served via terminal services. Company is not currently utilizing terminal server for remote access.

3. **Server Environment**

**Critical** – One of the two servers has the latest service pack from Microsoft installed. An update policy should be in place to ensure that all servers and server applications are updated on a scheduled basis.

**Important** – There is currently only one Domain Controller on the network. Microsoft recommends multiple domain controllers for both load balancing and for redundancy.

**Best Practices** – Servers are not located in a separate “Server” Organizational Unit, they are hosted with all other computers on the network. Servers should be separated so workstation policies to not apply to servers.

4. **Backup Environment**

**Critical** – The backup strategy that is in place is moving data over the internet. In addition to data backups, it is highly recommended to have disk backups that support bare metal restores. This enables us to recover from failed hardware much easier and quicker than typical data restores.

**Critical** – There is currently no disaster recovery plan in place. Although this plan does not need to be highly complex, a plan is necessary to ensure business continuity.

5. **IT Department**

**Important** – Documentation, process and procedure should be established for all critical systems, disaster recovery, etc.

**Best Practices** – Currently there is no process for deploying workstations within Flatrock Compression. Through the use of Microsoft RIS or a third party application such as Symantec Ghost, computers can be deployed from a previously created image, greatly improving efficiency when deploying new workstation or resolving issues.

These are only examples of findings intended to give you a better idea of the types of issues we typically uncover. If you feel that none of these examples apply to your business, keep in mind that they are only representative of the most common problems we see. Your environment will have different issues—or, in some rare cases, we have NO findings except that the network is already configured according to industry best practices! In the one or two perfectly-configured businesses we’ve assessed, we simply present this finding and the business thanks us for providing an outside opinion and peace of mind.

To schedule your assessment, call us today (713.533.8066) and we’ll set up a time that’s convenient for you!