THE DANGERS OF AN UNSTABLE IT INFRASTRUCTURE

By Jeffery Daigrepont, Senior Vice President | Coker Group

Do you ever wonder how the same software can perform exceptionally at one location and create chaos at another? Does your vendor ever claim that no one else is having the same technical problems like yours? Do you feel frustrated when the software vendor, the hardware vendor, and the support vendor start pointing fingers at each other—or at you? Realistically, there are only four possible causes (or a combination of all four) that will make an information technology (IT) ecosystem perform poorly, and the blame game typically goes in this order.

1. Improper training of the end-users
2. Software is defective
3. Software is improperly installed
4. The infrastructure is unstable (viruses, low capacity, low resources, connectivity, etc.)

What would you guess is the most common of the four possible IT offenders? If you guessed number four, you are correct. Surprisingly, this factor is often the last place people look when investigating performance problems. One reason is that the people who set up the infrastructure are usually the same people investigating the issue. It can be challenging to grade your own paper and even more difficult to admit costly mistakes.

One of the underlying aspects of any successful IT ecosystem is the infrastructure. Some call the structure the "backbone" as it is what holds up the entire operations of any medical practice/hospital. Any major service interruption affects the whole IT ecosystem and all the links in the chain of operations, including cash flow. In some cases, a breakdown can create liability and exposure to serious security risk. The resolution to these problems is not always black and white and may require calling on resources at all levels to address the problem. Addressing these issues can also take extensive time and effort and is distracting. Time can needlessly be consumed by fixing things that are not broken rather than addressing the actual issues. For example, upgrading a wireless access point will garner little improvements if the connectivity is unstable. The infrastructure is a delicate ecosystem that depends on many systems to perform correctly; therefore, any assessment must consider all facets of the environment.

When Coker is engaged to do IT infrastructure assessments, we use the following checklist to guide our audits:

1. **Check Configurations.** Examine all configuration from active director to routers and switches. Particularly, we compare these configurations to vendor specification and manufacturers' recommendations.

2. **Check Use of Monitoring Tools and Utilities.** Often, the systems will have internal monitoring tools and auditing logs of issues and failures. Reports can be generated from these tools and used as a starting point or first clue on where to look for problems.
3. **Check Server Capacity.** Many problems stem from servers being overloaded and/or exceeding capacity.
4. **Check Security Policies and Existing (known and unknown) Threats.** The system may have a virus or intrusion that is resulting in poor performance.
5. **Check for Conflicts in Configurations.** When multiple vendors are involved, each vendor may adjust configuration based on their preferences without considering how it might impact other systems.
6. **Check for Standardization.** A non-standardized IT environment is a nightmare to support and manage. This status is easy to detect but can be expensive to remediate as it may require replacing equipment to achieve a standardized environment.

Once our Coker team completes the audit using the above checklist, we run a comprehensive scan of the network and all of the devices attached to it. We also attempt to penetrate the network, just as an outside hacker would test all of the security policies and configurations. These exercises include social engineering and phishing scams, which will attempt to compromise an end-user into providing access. Nonetheless, NO amount of IT security can prevent a person from making (or being tricked into making) a wrong decision. Many hacks come from compromising staff members into giving up their passwords. Or in some cases, a staff member is compromised outside of the work environment. Here, the hacker assumes they use similar credentials at work, and in MOST cases, they DO! Therefore, safe testing of the staff is the best way to ensure everyone is aware of these threats.

A stable IT infrastructure delivers enormous benefits to the leadership of business-critical applications because it keeps the provider productive and the complaints to a minimum.

Coker Group would be delighted to help your organization evaluate your IT infrastructure. For a no-cost/no-obligation/non-biased consultation on strategies for developing a stable IT infrastructure, call 678-832-2021 to speak with Jeffery Daigrepont, Senior Vice President.