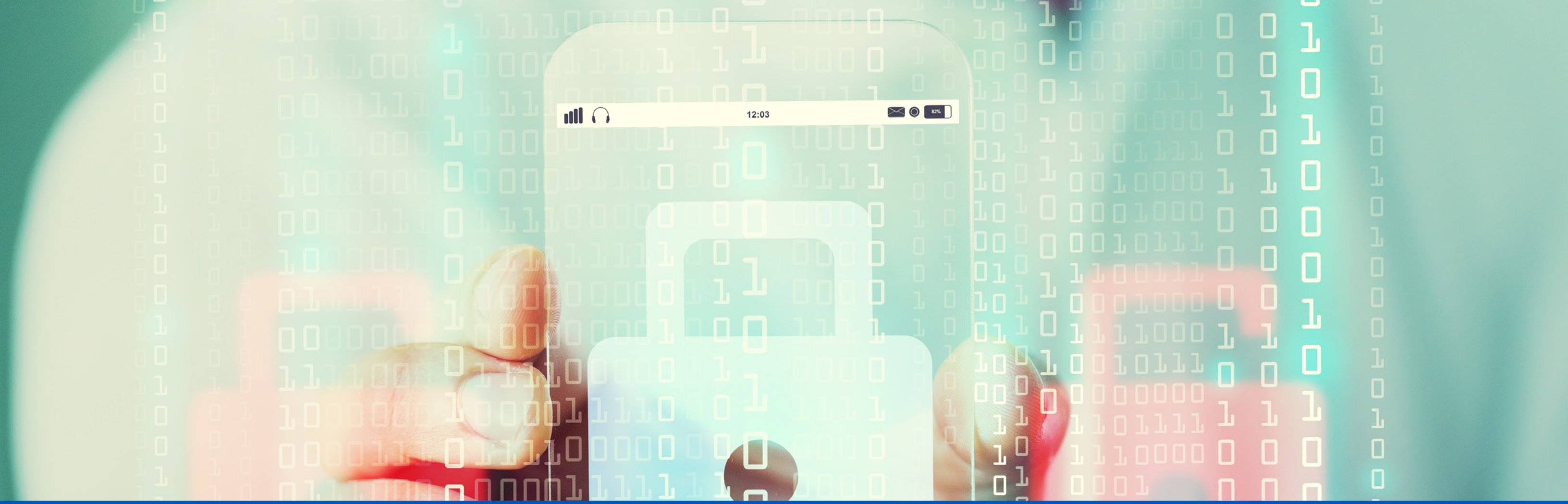

DynaSis

IT for the C-Suite - Quick Read Series
Modern Business Technology Education for the C-Level Executive

By David Moorman - President, DynaSis

Availability – Security – Mobility

When it comes down to it, availability, security and mobility are the hallmarks of a properly functioning IT system. How can you insure that you are protecting your customers, your employees and your business? Each of these topics is worthy of a detailed in-depth study by your IT team and most certainly the involvement of your managed IT support company. To get you started, here is an overview of all three.

Availability

If your system isn't available, you may be losing business, current and long-term customers, and/or employee productivity…all of which translate to losing money. If customers can't buy from your online store, they will go somewhere else. They may never come back. The time your employees lose can never be recovered.

So, how do you evaluate your IT network's availability? We look to "The Five 9s". Absolute perfection in anything involving technology is unlikely, but the five 9s means looking at a goal of 99.999% network uptime. What does that come to? There are 86,000 seconds in a day, and 31,536,000 seconds in a year (525,600 minutes), 99.999% uptime equals a mere 5.25 minutes downtime for the entire year. That's important to consider because while 99.9% uptime (1% downtime) may sound good, that actually comes to about nine hours downtime a year (or 10 minutes on average per week). A lot can happen in nine hours, especially if it is spread out in multiple failures. So how do you get to 99.999%. Here are four best practices that will help:

1: Evaluate Criticality – To develop a proper strategy, you must perform an IT Network & Risk Assessment that includes the evaluation of your current network, along with the calculation of the cost of downtime for each of your IT components. This includes determining your Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO). You should also include the likelihood of human error vs. equipment failure. Explaining to corporate execs what you are trying to accomplish in terms of revenue and customer loss prevention can be far more effective than simply telling them how much you want to spend.

2: Think in terms of service continuity along with disaster recovery. While disaster recovery planning is critical, and please do not think we are downplaying it, disaster avoidance can be augmented by creating a service continuity catalog that places the elements of your system in tiers of relative criticality. Since a particular element failure does not necessarily mean entire system failure, certain elements can be deemed less critical with different RTOs and RPOs.

Ensuring your technology is always available to you

Protecting your organization from threats around the clock

Allowing access to your data from anywhere, at any time, on any device

3: Availability should be measured from the perspective of the end-user. RTOs and RPOs must take into account both planned and unplanned downtime as it affects many people in the organization. IT teams must be aware of the needs of the various internal corporate constituencies: sales, marketing, R&D, procurement, distribution, etc. End of month for sales teams are obvious, but other departments may have needs that are less so.

4: Think in terms of availability and continuity when developing and testing new applications. Dealing with these issues AFTER development is often the norm and this can have a highly negative affect long-term. Unless given thought during development, your hardware may limit both availability and continuity.

All four of the Best Practices shown above are best served by an IT Network & Risk Assessment performed by a qualified managed IT support provider, and the involvement of members of various departments across the organization. Just remember, different groups have different needs and a full analysis of these are critical in developing an "availability roadmap."

Network Security

Network security is another big topic. Effective security requires a multi-layered approach and for the scope of this article, we are outlining a number of the aspects you should consider.

Access Control: Strictly enforced security policies are critical. Believe it or not, the majority of cyber intrusions are caused by the intentional or unintentional acts of employees. In addition to proper security policies, keeping non-compliant devices off your network is also extremely important.

Anti-Virus / Anti-Malware Software: Good anti-malware programs identify malware as it enters your system and kills it, and then, just in case something does get through, continues to monitor for those viruses, worms, trojans, ransomware, etc., that are rigged to sit dormant for days, weeks, or months before being triggered.

Application Security: Software needs to be protected…all of it, whether you build it or buy it off the shelf. Any application, no matter how well thought-out, can contain vulnerabilities that hackers can use to attack your network.

Data Loss Prevention: There are technologies that can prevent your employees from sending sensitive information outside of your network. This is something that sometimes happens inadvertently and sometimes intentionally. Either way, it is something you want to prevent.

Email Security: This is the number one threat to the security of your network because of sophisticated phishing campaigns, including social engineering tactics, that cyber-criminals use to trick unsuspecting employees into giving away information. Email security can be greatly bolstered through use of security programs that identify incoming attacks that then prevent the distribution of sensitive information through outgoing messages.

Firewalls: Whether hardware or software, firewalls create a barrier between your network and the outside world using a carefully designed set of rules that determine whether email traffic is allowed into your network or blocked.

Mobile Device Security: With more and more companies supporting proprietary company applications on mobile devices, these devices are becoming richer and richer targets for cyber-criminals looking for vulnerabilities. Additionally, many companies allow employees to use their own devices for company work, including accessing company files. High level management of these devices is critical.

Virtual Private Networks (VPNs): VPNs encrypt data using Secure Socket Layers (SSLs) to prevent its theft. Encryption is one of the most powerful tools a company can use in keeping data protected.

Wireless Network Security: Simply put, wireless networks cannot be as secure as those that are hard-wired, unless you implement stringent security measures using products that were developed specifically for this challenge. Without this level of protection, anyone sitting in your parking lot may have the ability to gain access and cause harm.

Mobility

Many people think of "mobility" as wireless connectivity, but it is much more than that. When you tie in cloud computing, it makes your organization more relevant, more immediate, not to mention more intelligent. Here are some of the ways that mobility is changing business:

1: We are not just connecting telephones, tablets and laptops, we are also connecting "things" through the Internet of Things (IoT). For companies using these "things", real-time data can prove very valuable for analysis in many ways. However, there may be serious pitfalls. Let's look at home security as an example. IoT devices that have come on the market to date generally are run by firmware, which is software installed at the factory and usually not equipped to be updated. Suppose your thermostat is such a connected device, with a vulnerability that allows hackers to read its history. Assume that during the summer, you set the main floor daytime temperature for 72 degrees and 76 for night time. When you go on vacation, however, you set it to 76 degrees for 24 hours a day. So, if a hacker reads this change he can assume no one is home and your house can become a target for theft. This is just one example, but similar events can take place not only in residences, but also in businesses.

2: Application Redesign. We are already seeing a vast changeover from systems solely designed for PCs to those adapted for smartphones, as well. Part of this changeover involves much shallower menu navigation. Instead of deep-diving menu structures, mobile users expect to reach their online destinations in just a click or two. On another front, the ability of mobile devices to sense where you, or your employees, are located will have far reaching implications on many industries. Think of how Uber and Lyft use such technologies to assign the car closest to the customer.

3: Portable devices lead to portable services. It has become standard practice today for people (including your employees) to use mobile devices to download, work on, and re-upload all sorts of documents. Because of this, mobile security has become a major issue. More and more, multi-factor, also known as two-factor, authentication is used to insure these devices are only used by those people authorized to do so.

4: Persona Identification. IT services will be developing ways to separate a person's business persona with his/her personal persona, and the various data and applications that apply to each. This technology will become an important supporting tool for the ever-growing "bring your own device to work" policies that many businesses either tacitly or purposefully enact for two reasons: 1) people do not want to be burdened with multiple devices, and 2) it is cost effective for the employer.

> *"Enterprise mobility is an approach to work in which employees can do their jobs from anywhere using a variety of devices and applications. The term commonly refers to the use of mobile devices, such as smartphones and tablets, for business purposes."*
>
> - www.TechTarget.com

If you want to learn more, give us a call, or fill out the form. We have been working with Atlanta's small to mid-sized businesses for more than 25 years and we would love the opportunity to speak with you. www.dynasis.com.