

Securing Networks to Increase Effectiveness of Organizations

Brian Sheehan, Vice President of Network Systems & Support, DelCor Technology Solutions

A network's security is a major key to its effectiveness. Exposed pieces of infrastructure, poor awareness of systems' status, absence of monitor/alert systems, and overworked support staff are all leading causes of IT failures in organizations today.

For a long time, these issues have been a fact of life for end-users who have grown accustomed to finding work-around solutions to minimize data and productivity loss when a system is either down or crashes. During this time, network security could only be accomplished by staff manually updating a virus list, monitoring a network for intrusion, or responding to issues without being immediately alerted to the source of them. Not only did this form of security expose an organization to human error, but it also led to an IT staff that was no longer working to improve their organization's ability to deliver value. In cases like this, IT became simple troubleshooters – not innovators, which is where organizations can start to see real value from its IT costs.

In a marketplace where there is constant competition for attention of constituencies, it's imperative that an organization continues to improve on its ability to deliver value. As a level of security is established which allows staff to stay productive, systems to stay online and available, and IT staff to focus on innovation, IT achieves a higher level of value in the eyes of the organization and its constituents.

Organizations that aren't focused on turning a profit have different needs, constraints, and concerns than those that are focused entirely on their bottom line, and can have a hard time finding a security plan that fits them properly. This paper will lay out the key steps that nonprofits should take in order to secure their networks and ensure that their critical systems are uninterrupted. In taking these steps, organizations will be moving from a reactive network security state to one where their network is proactively protected, defended, and quickly fixed so that they spend as much time as possible working towards their mission.

Assumptions

Prior to discussing these crucial steps that every organization should undergo, it's important to examine a few general policies that every network should be operating under:

Established Network

The American Society of Association Executives reports that 32 percent of associations are still operating in a standalone or peer to peer network configuration.¹ It's important to realize that while this might be an acceptable solution for some smaller organizations, it does not constitute a network and makes it difficult to protect critical data and systems. Functioning in a client-server environment is a key first step before deploying these suggested security practices.

Network Perimeter Security Tools:

- Firewall
- Anti-virus
- Anti-spam
- Patch management

Automatic Monitoring:

- Monitors perimeter & critical systems
- Can also monitor physical environment
- Minimal risk of human error

Support System:

- Support team responds on as-needed basis
- Better directed to source of issue
- Able to correct issue quickly & return to other duties

Reliable and Stable System

Servers run and store the critical applications and data that an organization needs to be successful. They should be recently deployed (within the past three years) and should be constantly updated with the most current version of the operating system and patches. Failing to establish this minimum standard in an organization's technology can lead to many more network issues than simply ones based around security.

Physical Security

This is the ground point in securing a network. At the bare minimum, the servers that a network resides on should be housed in a secure location, which can be as simple as a designated room in an office or as complex as an enterprise level data center. Generally, all of these locations will have a secured entry system along with fire suppression, backup power, and power surge protection for the hardware. This guards the network at its source and wards off attacks that can be launched by physically patching-in to a server.

Security: The Foundation of a Successful Network

At the root of a successful network is security. Security establishes the foundation upon which IT can grow and add value to an organization. The three steps to establishing this foundation are:

- Installing security tools and systems to guard the perimeter of the environment
- Deploying automatic monitoring systems to alert to any breach in the system's security or failure in critical systems
- Instituting a support staff that focuses on responding to security and system failure alerts on an as-needed basis

Network Perimeter Security Tools

A new proactive security posture begins with establishing an outer perimeter from the global Internet with security

tools and systems. Critical tools that are usually included in this group are:

- **Firewalls** – The first line of defense. Establishes and protects the border between the network and the open Internet.
- **Anti-virus** – Continuously monitors network and systems for harmful pieces of code that can erase data or render critical network and systems unusable for a significant period of time.
- **Anti-spam** – Guards email systems against unsolicited email messages that reduce staff productivity and that can pose security risks in the form of viruses attached to messages. With 50 percent of today's email traffic being caused by spam, it's critical to take steps to guard against this constant threat that could lead to a significant loss in productivity.
- **Patch Management** – Closes loopholes in operating systems and programs already installed on servers and end-user systems. A patch management system automatically downloads, tests, and installs new patches for programs and systems as they become available with minimal manual management. Being an automatically-performed operation, it also is not exposed to common issues rising from manual deployment of new patches.

These tools are held together by global policies which govern the usage of the network. These policies establish, among other things, standards for accessing the network, which can be varied, based on whether a user is accessing the network remotely or while onsite at the organization. Typically, organizations will utilize different policies for remote users and users onsite.

These tools and policies establish a network's perimeter security system. Each piece to this system plugs a critical hole in a network that can be exploited by an attacker and leave an organization completely exposed.

Automatic Monitoring

Automatic monitoring systems support

the perimeter protection that guards an environment from intrusion. Monitoring systems can be setup to watch over Internet connectivity, intrusion detection, critical systems availability, and the internal network environment. Often overlooked, but equally as crucial is the monitoring of the physical environment that houses a network. Monitoring systems can also be setup to observe and alert to critical changes in temperature, unauthorized access, and water emergencies.

Having these systems in place provides critical knowledge around how a network is performing. An automatic monitoring system will alert a support team to breaches in security or if critical systems fail, allowing the team to respond more quickly to network issues – before it hurts an organization's productivity.

While monitoring can be accomplished using manual processes, the cost to an organization can be astronomical when considering the risk of human error. Manual monitoring is susceptible to large-scale issues including critical failures and significant downtime as a result of an individual error by a technician.

The costs and risk associated with manual monitoring processes are immediately reduced when implementing an automatic monitoring solution. Automatic monitoring uses servers that continually scrutinize a network and offer this oversight without the risk of error by a technician.

Support System

Issue remediation is a critical part of getting a network back online when a security breach occurs or a system fails. Technicians that are alerted to these breaches or failures by automatic monitoring systems are provided with specific problem information enabling them to focus-in on the problem and quickly respond to get an environment online again.

By using a support team that responds to alerts produced by an automatic

monitoring system, the team is better directed to the source of the issue and is able to reduce troubleshooting missteps. This limits the amount of unscheduled downtime that the organization is forced to deal with during this failure.

In addition, by better directing IT staff to the immediate source of the issue, they are able to correct the problem and return to what should be their main focus: innovating and improving the way that the organization can lever-

“With 50 percent of today’s email traffic being caused by spam, it’s critical to take steps to guard against this constant threat... that could lead to a significant loss in productivity.”

age technology to deliver value to its constituency.

By using a support team that responds to alerts produced by an automatic monitoring system, the team is better directed to the source of the issue and is able to reduce troubleshooting missteps. This limits the amount of unscheduled downtime that the organization is forced to deal with during this failure.

In addition, by better directing IT staff to the immediate source of the issue, they are able to correct the problem and return to what should be their main focus: innovating and improving the way that the organization can leverage technology to deliver value to its constituency.

Online Backup for Business Continuity: When All Else Fails

As a foundation of information security is built within an organization using tools, systems, and staff, it’s also important to establish procedures that can be used when one of these pieces fail. If a server fails, it can easily cause a loss in data – this can be member information, business records, or other pieces of information critical to the suc-

cess of an organization.

Irrecoverable data loss can be crushing to an organization, which is why many successful ones are adopting business continuity (BC) plans. This plan generally involves a data backup and restoration system that enables an organization to restore lost data following a disaster on the network. Disasters can include more than simply a hurricane or earthquake – staff errors causing accidental deletions, power failure, internal flooding, and hardware failure, are all

examples of disasters that can put an organization at risk of losing data that’s critical to its survival.

Most best-practice backup solutions involve data being sent over a secure Internet connection to a secure, offsite location. While tape backups have previously been the standard in organizations, they require human intervention and are susceptible to human error. The key is to use an automatic system that backs-up data at specific intervals and sends it offsite so that it’s not affected by a disaster that might plague the original network. Using an online backup system provides an organization with a safety net that ensures that previously defeating errors will not threaten its survival anymore.

Achieving a Higher Level of IT

The mission of IT is to serve its organization and improve the pursuit of its goals. Establishing a foundation of security for the network provides the level of reliability required for IT to be able to shift its role into being a resource for its organization and no longer simply fighting fires, which is an IT state that plagues most organizations today.

As an organization increases the effectiveness of its IT environment, the focus of technology moves from being an internally-focused conflict remediation group to a resource that is leveraged by the organization as a whole to provide a higher level of value to its constituency.

Conclusion

Organizations can no longer function on haphazard approaches to securing their networks. They must take steps that shift them away from a state where they reactively respond to security issues, to one where they proactively guard against issues before they occur. On the off-chance that they do occur however, successful organizations will support their perimeter security with monitoring systems that automatically alert to breaches in the network or critical system failures. As organizations implement these steps to establish this security foundation that will support further innovation on their networks, they will be able to further-leverage IT in order to increase and improve the value that’s received by their constituencies.



8380 Colesville Road, Suite 550
Silver Spring, MD 20910