# The seven domains of a typical it infrastructure

Government

User - The User Domain is the critical backbone of our network and we must pay close attention to user activity and shape user behavior on our network. I list this as a high priority due to the fact that it is the one that will most likely open up threats on our network from file downloading and surfing the web. My proposal for a solution for this would be to restrict web browsing to only required users. This will allow us to focus our concentration on those users, monitoring for potential network vulnerabilities.

I also suggest we implement a basic training course on the proper use of sensitive data and best common computer practices. Workstation - The Workstation Domain is where we can focus our energy on maintaining a clean network. We should do nightly anti-virus scans which will report any found issues back to the IT Department. This will then allow the IT Department to track down the user responsible for infecting the network and allow us to pursue corrective action. LAN - For the wired portion of our network, I propose a few solutions that will help secure our network.

First we will need to ensure the safety of our equipment from tampering. We should have all switches and sensitive equipment (i. e. Servers and Network Attached Storage (NAS) Devices) in a room that is locked at all times. If available, we can use a card access system to monitor employees that gain access to this portion of our network. Wireless connections open our network to potential threats. We should do everything possible to limit the number of allowed wireless devices on our network. I suggest that we enforce a policy of aprimary and secondarywireless network.

This would allow us to give our employees the functions they need while maintaining a secure network. Our primary network will be secured with Wi-

Fi Protected Access version 2 (WPA2) and the user of a complex passphrase to prevent brute force attacks. This section of our network will have a limited number of users allowed, with each users activity being closely monitored. The second wireless network will be an isolated network which will allow all approved employees and clients to gain outside access on their mobile devices, without compromising our network.

Another step would be to implement security on the network side by locking down each switch port to a specific mac address. This will help circumvent someone from removing the cable from a computer and plugging in another device. While this doesn’t completely eliminate threats of that kind, it will lessen the chance of having an unknowing user infect our network with a virus brought from another destination. LAN to WAN - The bridge between our outside network or WAN to the internal network should be monitored closely.

As mentioned in the WAN section above, we should focus on restricting access to our network to help prevent unwanted attacks. I suggest that we implement a hardware firewall on our network. A hardware firewall will give our network a much needed layer of security against potential threats. WAN - For this domain I suggest that we implement Virtual Private Network (VPN) servers for any of our employees or clients that are trying to access our network remotely.

We should also ensure that all unused ports on our network are blocked which would help limit attacks on our network. We should approach it from the stance of what we need, not what we do not need and start our outbound firewall with all ports closed. Only open the ports that are needed to have

our network function. Remote Access - The Remote Access Domain should be monitored closely with each connection and activity extensively logged. Allowing access to our network from an outside source, opens up many possible threats to our network.

I suggest that we create a separate server and network for our remote access, keeping it isolated from our primary network. We could implement server and storage mirroring for both networks. This would allow employees to work on projects from a remote location, or clients see the progress of project and not put our network at risk. Systems/Applications - Since the system/ application domain consists of all of a business's mission-critical systems, applications, and data it is important to ensure that this domain is secure at all times.

Failureto do so will result in large amounts of sensitive information as well as the threat of having productions cease to function. Unauthorized physical access is gaining access to a physical entity without permission. This is potentially dangerous because if an individual were to gain such access they could destroy the systems and data within the systems. This threat is centered on access to such places as data centers with a great deal of sensitive information. To prevent unauthorized physical access policies, standards, procedures and guidelines must be followed.

For example, all guests must be escorted by an employee at all times. Staff should immediately report any suspicious activity and question persons that do not have an employee ID or badge visible. Data loss occurs when any stored data is destroyed. This is considered the greatest risk to the system/ application domain. To combat data loss, backups should occur regularly.

The backups should be stored at an off- site location to allow full data recovery in the event of data loss.