Phone: 253-244-3401
Email: Info@dunnco.net

DunnCo Diversified Services LLC

White Paper
Security Awareness – The Threats from Inside

In The Lord of The Rings Saga, King Theoden and the people of Rohan are safe in their castle at Helm's Deep, and are holding their own against the enemy, until the one vulnerability of their castle is breached when a bomb is carried beneath the walls of the castle through a drainage tunnel.

Your network can be looked at the same way. You have a strong exterior, and it is well guarded. But there are spots which, if exploited, can open your entire enterprise to a data breach, or worse.

In today's world, your business relies on technology in almost every facet of your operation. Can you afford to lose data, or worse, the time and loss of business associated with a cyber security incident?

Here are five things you should know about and make sure you have buttoned up tight so you'll sleep better knowing your cyber defenses are guarding the gates while you're resting:

Your Network Firewall

If you think of your network's firewall as the front door of your network, you can see how vital it is to the security of what it protects. Most firewalls ship in a completely "locked down" state, and its up to the user to "unlock" or allow the services and traffic that they need to pass through the firewall. Still, it's a good idea to inspect the firewall from time to time and make sure it is still operating in alignment with your business' requirements.

Anti-Virus Protection on Every PC

Computer viruses and "worms" today are largely detected and prevented from doing their dirty work by effective and updated anti-virus software. The key is keeping your anti-virus software updated on EVERY PC in the enterprise. While keeping track of this on all the machines in your environment can be tedious, it is *vital*. If your business is running more than 3-5 PC's, I recommend using a centralized tool to manage all of the PC's from a "single pane of glass". A centralized approach will insure you've got your anti-virus protection doing its job at every station.

Anti-Malware Protection on Every PC

Anti-Malware software is the second ingredient in the prescribed "cocktail" of protection for every PC in your business. "Malware" comes in many flavors, from innocuous and barely noticed to dangerous and crippling to your PC, and potentially your business. On the innocuous side, some websites load tracking "cookies" into your browsers that send data back to their "mother ship" to let it know about your browsing habits, and other "infobits". On the really nasty end of the spectrum, you may find that your PC has been completely taken over by "ransomware", that demands money or a credit card payment to unlock your data. If you're lucky, this hasn't spread beyond the one PC onto a server or your corporate database. If you've been attacked at this level, it's highly likely that you'll need professional help quickly to get your systems cleaned up and your data intact. Just like anti-virus software, anti-malware software should be kept updated, and should be set up to run regular scans on your PC's.

Phone: 253-244-3401
Email: Info@dunnco.net

Appropriate Controls to Deal with External Programs on Every PC

In a recent episode of the TV Show "Mr. Robot," hackers are attempting to gain access to the security and controls network of the Rikers Island Prison in New York City. Since they know that getting past the firewall from the outside is a labor intensive and detectable act, they send one of their team through the staff parking lot dropping USB thumb drives all over the ground. Within minutes, a guard picks one up, when he arrives at his desk inside the prison, he pops it into his PC, and plays the little "game" that came on the drive. While this seems harmless enough, while he was playing the game (actually a Trojan Horse), the prison's network was being scanned, and hooks were being installed to allow the hackers to control the whole facility. Does this sound farfetched? Yes it does, but in the real world, the security firm Symantec did exactly the same experiment in the parking lot of a major fortune 500 company. Within 2 hours, enough of the USB drives had been installed onto corporate PC's to bring the enterprise to its knees, had it been an actual hack attempt.

Does your staff take work home on thumb drives? Do they bring these drives back the next day? Are their PC's at home protected with up to date anti-virus and malware protection? Has something unwholesome attached itself to the USB drive?

Email attachments that look legitimate, but open up programs that install themselves on the PC are also threat vectors that allow the bad stuff onto your network. It's like opening the front door and saying "come on in!"

Security Awareness – "The People Factor"

In nearly every case of external programs that wind up installing themselves on PC's, they get there through the direct assistance of a Human Being. This is known as "social engineering." So, what kind of anti-virus and anti-malware "software" can we install on the human beings in our midst to prevent them from unleashing chaos onto our networks? It's called "Security Awareness Training." Beyond the obvious first steps of having and enforcing an AUP (Acceptable USE Policy) for your computers and network, Security Awareness Training for your staff will help them be better prepared by "looking over their shoulder" and questioning the various ways that the nasty bits are trying to use to get onto your network.

Your Security Awareness Program should cover the following areas:

1) Safe Web Browsing
2) Phishing Emails
3) Social Engineering Attacks
4) Safe Home Computing
5) Effective Password Management
6) Instruction on how to "Break Glass In Case of Emergency"
7) Warning Signs that a hack or breach has occurred

Once you have your "castle walls" fortified, and your users educated, you stand a much better chance of riding through the storms of cyber security breaches and threats.

For more information on receiving a no obligation free one hour training seminar at your location on Security Awareness, contact DunnCo at 253-244-3401 or by email at info@dunnco.net