The Tonalli Group LLC

SUMMARY

Where is the balance if any between corporate level IT security and the plethora of consumer hardware and software interfacing with the corporate network? Such consumer devices are known to cut IT costs and boost innovation. What are the pending threats, strengths, opportunities, and weaknesses for corporate level IT security versus hacker intrusion, and the innocuous and not so innocuous employee introducing consumer devices and software?

Marcos Abeyta, PMP
Branch Chief- Competitive Intelligence & Business Intelligence

IT Corporate Security: Innovation & Productivity Versus Data Loss & Hacker Intrusion

The Tonalli Group LLC
Denver CO & Albuquerque, NM
www.tonalli.com

1.0 Introduction

iPod, iPhone, VOIP, Gmail, and many others all are opportunities for data loss and hacker intrusion, yet all are readily available consumer devices that can improve collaboration, innovation, and reduce IT costs. Yes, such innocuous devices such as media player phones and Nintendo Wii pose threats, so how does the corporate IT secure the network yet promote employee collaboration and innovation with minimal risk and threat.

2.0 Smart Phones

American Airlines banned its' employees with iPhones from interfacing with the corporate network. Why? Security or lack thereof. The iPhone simply did not meet the corporate level security requirements of AA. Not all devices are approved for interfacing with the network, nor should they be.

2.1 What to do?

Each company must have an up to date list of approved devices, preferably before or within days of hitting the market. Assist the employee and IT by either supplying or subsidizing the cost of the approved device. If the company does not assist or promote, then there is the threat of an employee introducing a rogue or unapproved device.

3.0 Laptops

Data loss and intrusion via laptops has certainly been a losing battle for many organizations. Recall the recent headlines of the Veterans Administration and Pfizer, and this concern and threat potential is well founded. Laptops portability and size combined with an abundance of USB ports, wireless ports, and other openings make this an easy target and huge threat.

3.1 What to do?

For starters, beef up the software security on the laptops. Use double authentication when connecting, and disallow any connection that does not have the latest security updates. Possibly use de-perimeterization, or do not allow the laptop user to access information within the firewall. Besides, information within the firewall is not essential for simple collaboration and communication. Also consider subscribing to services such as Computrace LoJack and peripherals such as the Yoggie Gatekeeper.

4.0 VOIP

While this may have been a godsend for reducing telecommunication costs and improving collaboration, security threats abound. Every time a VOIP is activated, it sends out a ping or registration on the network calling attention to itself. Hackers can listen for this ping and eavesdrop, or even overload the network with their own cloned pings. Hackers can then redirect calls or charge others for hacked calls all while on your network. Moreover, knowledgeable hackers can find VOIP configuration information on the web.

4.1 What to do?

There is no single vulnerability, therefore there is no single solution other than disconnecting the VOIP. Research is underway by both vendors and users to address some of the vulnerabilities. This one will have to be monitored closely.

5.0 Do's and Don'ts.

5.1 Do

Allow and grant employee access to the latest consumer technology, yet robust devices and software only**.** Create policies and procedures regarding consumer devices. Remember to keep it up to date. Rethink security, create pilot programs to see what works and what does not. Sometimes less is more, and will save on IT costs. Sometimes consumer devices work better and are cheaper than corporate grade devices.

5.2 Don't

Don't stop everything and ban all consumer devices from the network. Rather, seek to understand which employees are using it and why. Don't treat employees like nincompoops. Some are actually quite tech savvy and can assist, but figure out who is ready for the challenge. Don't skimp on storage or employees will start using services such as GMail. Don't forget to educate and train employees. You do not want data loss or intrusion due to human error.

6.0 Find our more

Consumerization Working Group
International Computer Driver License
Jericho Forum
BlackHat
See the Slide Show at www.tonalli.com

Marcos Abeyta, PMP
Branch Chief- Competitive Intelligence & Business Intelligence