BYO-INSECURITY TO BYO-SUCCESS

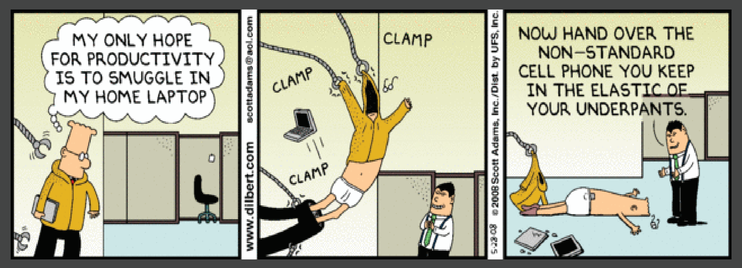
COIT TECH SUPPORT

Blurring of work and personal devices
Facebook = 50 % of all mobile data in the UK
Two or more devices per person
How to address the multitude of devices?
Anywhere Anytime Access….
Cloud security implications
Consumers expectations of network speed and access
Multicast traffic impacts networks
Consumer type tech support model
Bypass IT deprartments

USER MISTAKES

Failing to lock down device
Not having updated (and most secure) apps
Storing sensitive, data on unauthorized device
Opening questionable content
Not adhering to company's social media policies
Not encrypting employees' devices
Using public or unsecure WiFi
Lack of understanding of metadata

NO CONTROL FREAKS



More Resources @ http://networkpaladin.org

HAVE A PLAN

Determine how technology will be used to meet those desired outcomes
Then pick the specific technologies/apps
Look @ policies and infrastructure
Does your AUP include mobile devices
Who is responsible for device security
What security do mobile devices need?
What are the policy issues to be considered?
How network loads can be predicted
What can be done to control the network demand ?

THE A - TEAM

TEN+ COMMANDMENTS

Thou shalt: Set desired outcomes first
Thou shalt: Have ongoing communication with stakeholders -- Use surveys
Thou shalt: Create thy policy before procuring technology work with HR
Thou shalt: Invest time and money on staff training
Thou shalt: Hold sacred personal information
Thou shalt: Implement management solutions
Thou shalt: Protect data not devices
Thou shalt: Monitor thy flock—Herd automatically
Thou shalt: Part the seas of complacency by building ownership and support
Thou shalt: Invest in network infrastructure and access to digital resources
Thou shalt: Implement the controls necessary for work
Thou shalt: Plan for continuous evaluation - funding

KEY FACTORS

Enforce Long passwords
Perform periodic audit
Encrypt local storage / mobile device
Enforce the use of (filter/bandwidth limits)
Enforce wireless security policies
Backup and recovery of confidential data
Centralized configuration and software upgrades "over the air"

SMOOTH DATA FLOW

Capture real- time data, log, flow and automate reports
Analyze, Analyze, Analyze
Security Onion
Packet shapers
Splunk (paid) or ELSA (Open Source)
ELSA how to http://tiny.cc/904p6w

MDM CONSIDERATIONS

Manage policies
The ability to roll out apps to users
Manage updates and installs
Inventory mobile devices and their installed software
Quickly identify devices that have violated AUPs

A good list of MDM solutions and what they offer
http://www.enterpriseios.com/wiki/Comparison_MDM_Providers

VISIBILITY

Eyes in the Sky
Must be able to see what is happening in the air (Wireless) and take actions before it hits the wired network lines

Use VLANS to separate traffic types and users

Feet on the Street:
And the wired infrastructure must be able to handle increased traffic

Network Monitoring
Oppsview

City of Chattanooga
IT.Security
Compiled By
Ernest Staats