MOBILE IS HERE TO STAY, SO HERE'S HOW TO BE READY

Dean Weber
Chief Technology Officer
CSC Cybersecurity
May 15, 2012

One Cloud Model – Apple iCloud

Personal NOT corporate solution

(but corporate data may be on it)

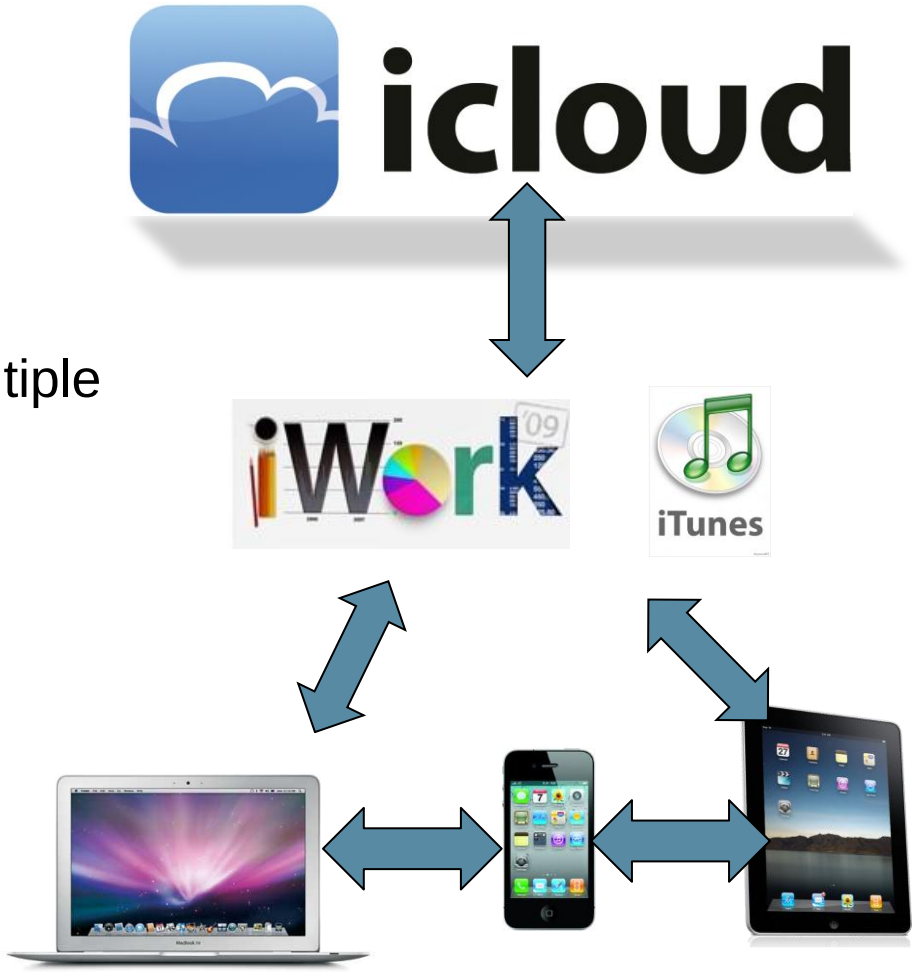
Goal is adoption of cloud concept

- Sell iOS devices
- Make iWork and iTunes “sticky”

Data resides on cloud AND on multiple devices

If adopted, user is stuck with

- Apple computer
- iWork software
- iTunes music
- iCloud storage
- iEverything



Virtualization + Tenancy + Outsourcing = Cloud = Mobility

- Cloud and cloud like environments enable and require mobility
- Data, applications, services reside in cloud
- Require ubiquitous, reliable, and SECURE access
- Require authenticated access
- Require security of data at rest and transmission
- Enable Bring Your Own Device (if done well)
- BUT requires emphasis on security
  - Network security
  - Authentication
  - Device(s)
  - Applications
- Is mobile security up to the task?

Users Want Open Access

- **Open**
  - Employees can use private/own device without restrictions
  - Access to corporate assets (E-Mail, calendar, documents) via separate app installed
- **Moderate**
  - Strict separation of personal & business data
  - Restriction of security relevant functions & apps (camera, games, legally dubious apps, enforce key lock)
- **Restrictive**
  - No private use of device, only business data & apps
  - Full device encryption, no access to open internet & application markets (iTunes App Store, BlackBerry App World, Android Market)

Must consider deployment, maintenance, security and cost control

- **Device Security**
  - Password policies
  - Device encryption
  - Port control (WiFi, Bluetooth, ...)
  - Remote lock & wipe
  - Email access policies
  - Wipe application data
  - Selective email data wipe
- **Asset Tracking**
  - Hardware & Software inventory
  - Extensive reporting
- **Backup / Restore**
  - Application data
- **Enterprise App Management**
  - Deliver and control
  - Blacklisting of applications
  - Install, update, remove or lock enterprise apps
- **Roaming Control**
  - Set data roaming policies
- **Process Automation**
  - Custom file transfers & movement
- **Device Configuration**
  - Profiles for VPN, WiFi, Email, ...
  - Disable Camera

Wireless Security Overview

- Karsten Nohl and Chris Paget taught us that mobile phone networks are not secure
- Cracked algorithm for GSM random channel hopping
- Able to intercept cell calls with device for $4,000 (and price declining)
- Attack at the cell provider or ISP level – NOT the user
- Cannot be detected
- No notification
- No defenses for data/voice in the clear

Active and passive intercept is common as attack devices are readily available

Two flavors of attack devices

A

Active intercept:
- Phones connect through fake base station
- Easily spottable (but nobody is looking)

B

Passive key cracking:
- Technically challenging
  - –Non-trivial RF setup
  - –Heavy pre-computation
- Allows hidden operation

Source: H4RDW4RE, DeepSec GSM training

Karsten Nohl - A5/1 Cracking H4RDW4RE

Wireless Security Overview

- Mobile phones themselves are in the Windows 2000 era of computing security (at best)
  - Only support one or two (at most) users & all has the equivalent of root access
  - Not learning from the mistakes of the desktop world
  - No popular phone has anything resembling a TPM
  - Design limitations skew towards user experience & battery life, not security
  - Smart phones connect to your network = attack vector + egress path
  - The list goes on and on…

Smart phones are mostly insecure computers with near constant connectivity

Wireless Security Overview

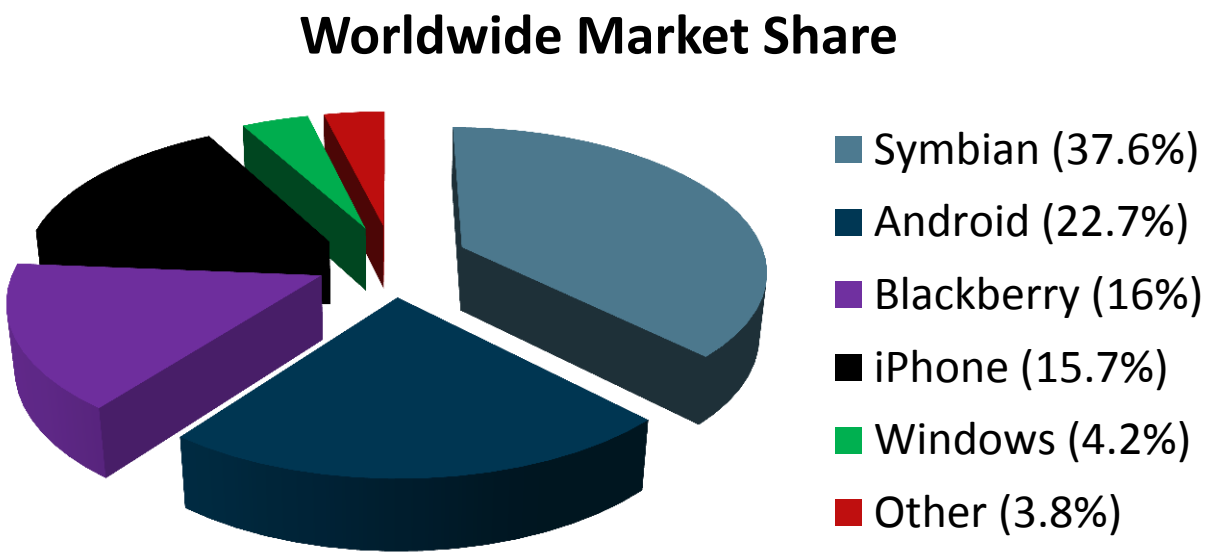
The alternative is ~~ugly~~ ~~complicated~~ ~~expensive~~ awful

530% larger and 250% heavier than iPhone 4

Wireless Security Overview

- The million dollar question:

How to make a commercial off-the-shelf mobile phone secure?



Reverse Engineering Conclusions – General

- **Large attack surface**
  - WiFi auto-connect
  - Browser bugs
  - Anything that worked on a computer ~~may~~ almost certainly works on a smart phone
  - Ask us in a month after we've worked out how to pwn the baseband
  - Physical access = game over
  - Bluetooth
  - Man in the middle
- **Mobile malware is becoming more prevalent**
  - Even 'legitimate' apps can leak data or access private information
  - New frontier for exploit & malware writers
- **Smart phones are forensics gold mines**
  - Email usually isn't secure
  - Cached GPS
  - SMS
  - Calls
  - Pictures
  - Cached keystrokes

ElcomSoft Commercial Data Extraction Tool

MAY 25, 2011 8:02 AM PDT

ElcomSoft to sell iPhone decryption toolkit

by Don Reisinger

Print E-mail

Recommend 21 Tweet 169 +1 0 Share 8 comments

A Russian computer forensics company, ElcomSoft, says it has developed a toolkit that can help law enforcement agencies quickly access encrypted file systems on Apple's **iPhone**.

ElcomSoft's toolkit is an important development as smartphone security and privacy have become a hot-button issue.

Last month, researchers discovered that the iPhone was tracking users' locations as they moved from place to place. The information was **stored in an unencrypted file on the iPhone**, as well as in iTunes backups. After privacy advocates complained that the iPhone was tracking user movements, Apple responded saying that it had no desire to track users, and the issue was simply a bug.

"Apple is not tracking the location of your iPhone," the **company wrote on an FAQ page last month**. "Apple has never done so and has no plans to ever do so." Earlier this month, Apple **released iOS 4.3.3 to remove the location-tracking feature**.

Other smartphones, including those running the **Windows Phone 7** and **Android** operating systems, also track a certain amount of location data.

Apple's fix could be a setback to law enforcement agencies, which for months have been **using iPhone and iPad geolocation data** in criminal investigations.

Enter ElcomSoft.

"This time around it's not about iPhone backups," ElcomSoft CEO Vladimir Katalov said in a statement. "Backups created with iTunes software already contain a lot of data, but not quite everything that's being stored or cached in iPhone devices. In contrast, we were able to break into the heart of iPhone data encryption, providing our customers with full access to all information stored in iPhone devices running iOS 4."

Gaining access to that data was no simple task. With the release of iOS 4 last year, Apple unveiled a new security feature for its mobile devices called **Data Protection**. That offering delivered hardware-based, AES-256 encryption on the iPhone 3GS, iPhone 4, iPads, and last-generation iPod Touch, effectively keeping the device's data, including SMS messages, e-mail, passwords, and other content, safe from malicious hackers.

"we were able to break into the heart of iPhone data encryption, providing our customers with full access to all information stored in iPhone devices running iOS4."
The Russian hacker tool will "extract all relevant encryption keys" from devices running iOS 4 and then used those keys to decrypt iPhone file system dumps…access to that content is possible even if the Apple product is protected by a password."

Reverse Engineering Conclusions - iPhone

- **The Good**
  - Difficult to get rogue apps installed without jailbreak
  - Jailbreaks/exploits are quickly patched
  - Can remote wipe—for a fee or via Exchange
  - Very popular, lots of vuln research
- **The Bad**
  - iPhone worm made people watch Rick Astley all across Australia

  - Local phone security / crypto is suspect at best
  - Once jailbroken, all bets are off
    - Difficult to determine whether phone is jailbroken
  - Lack of remote wipe without MobileMe or Exchange or other paid app
  - Very popular
  - Vuln researchers like it because it's so easy to find 0day
  - Reliant on Apple's cursory security checks
    - No real permissions except for GPS

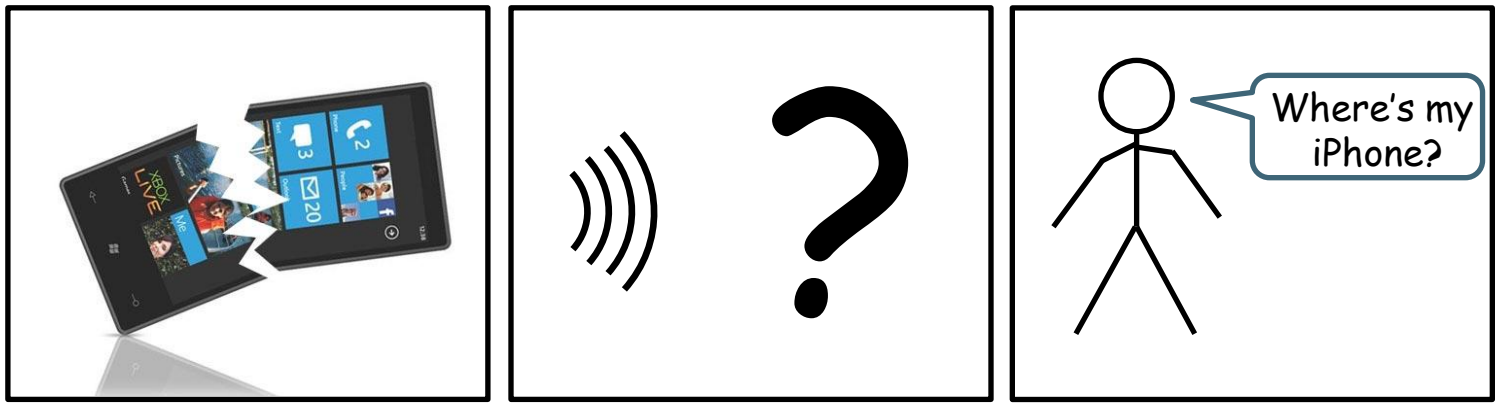
```
/*
  People are stupid, and this is to prove it so
  RTFM. its not thats hard guys
  But hey who cares its only your bank details at stake.
*/

// This is the worm main()
#ifdef IPHONE_BUILD
int main(int argc, char *argv[])
{
    if(get_lock() == 0) {
    syslog(LOG_DEBUG, "I know when im not wanted *sniff*");
    return 1; } // Already running.
    sleep(60); // Lets wait for the network to come up 2 MINS
    syslog(LOG_DEBUG, "IIIIIII Just want to tell you how im feeling");
    char *locRanges = getAddrRange();
    // Why did i do it like this i hear you ask.
    // because i wrote a simple python script to parse ranges
    // and output them like this
    // THATS WHY.
```

Reverse Engineering Conclusions – Android

- **The Good**
  - Open source means more people can work to secure it
  - Rapid improvement possible
  - SELinux variant already ported
  - Apps are sandboxed from one another
- **The Bad**
  - Decentralized app marketplace makes it easier to get malware
  - Susceptible to being rooted
    - Difficult to determine whether phone is rooted
  - Locked into the provider's version of the OS
    - X time between vuln discovery and vendor's patch
  - Hand rolling the OS can void the warranty
  - Apps get zero security screening
  - Apps only need to "ask" in order to do potentially malicious things (or anything for that matter)
  - Apps can be remotely installed using only Gmail creds

Reverse Engineering Conclusions – Windows Mobile 7

- **The Good**
  - Nobody is really using WinMo 7, so few are attacking it
- **The Bad**
  - Nobody wants a WinMo 7 phone (sorry, Nokia)
  - There are jailbreaks for it already, and GeoHot is taking up the cause



If a Windows phone is hacked in the middle of, well, anywhere does anyone care?

Sources: http://news.cnet.com/8301-10805_3-20029189-75.html
http://tech.fortune.cnn.com/2011/01/31/npd-android-os-phones-now-outsell-everyone-else-in-us-combined/

BYOD

- Device themselves are not secure
- No standard build
- No standard AV/Anti Malware
- No standard browser/config
- No standard OS
- No patch management = no patching
- Corporate data on personal machines
- Personal data on corporate machines
- Corporate data travelling across borders
- Credential/ID information on device
- Whole disk encryption/remote wipe

Enterprise Mobile Device Management (EMDM) Industry Challenges and Drivers

- With the addition of innovation devices and other industry leading OS's, overall platforms and carriers has proliferated over the past few years, creating additional challenges for IT organizations.

Enterprise Mobile Device Management Industry Challenges and Drivers

IT Challenges	Key Business Driver Examples
• Mobile device support • Device and data security • Applications deployment • Device control • Device deactivation • BYOD (bring your own device) • Email security	• Security and Governance Requirements (HIPAA, FINRA, FERC, SEC, etc.) • Mobilization of a business process (expense reporting, Salesforce automation) • Developing mobile applications and/or mobilization of a business process • Deployment beyond BlackBerry • Launching Tablets

Enterprise Mobile Device Management

What We've Learned…problems and causes

1

There are More Device Form Factors and OS Choices than Ever Before (users are blurring the lines between company/ personal data).

2

Consumer Based Trends and Preferences Will Continue to Influence Devices Used in Enterprise.

3

Mobile Devices - Personal And Corporate - Connecting to Enterprise Assets Need to be Managed and Secured In a Scalable Manner.

4

There are a Growing Number of Solutions Which Provide Varied Capability and Functionality (Email, DM, Security, TEM).

5

Enterprise Demand includes a Robust MDM and Messaging Solutions, But Have Varied Needs.

Enterprise Mobile Device Management

Meeting the IT manager and end-user needs

Acquisition and Deployment
- Cost optimization
- Multiple device and carrier support
- Image devices
- Application enablement & deployment

Lifecycle Support
- Inventory management
- Security policy compliance
- Issue resolution and troubleshooting

End-of-Life
- Data protection
- Device upgrades
- Recover/Reallocate devices

Service Delivery Choice
- Managed service option
- Multicarrier support
- Cloud hosted
- Developer support via APIs/SDK

Productivity
- Reliable access to corporate data and applications

Flexibility
- Choice of device
- Bring your own device
- Merging personal and professional use

Convenience
- Over-the-air troubleshooting

Enterprise Mobile Device Management
Key Drivers

- Management of mixed platforms/devices
- Carrier agnostic
- Protect Email
- Provisioning device enhances protection
- Application management
- Device monitoring
- Policy enforcement and notification
- Usage management
- Analysis and reporting

A Centralized View - Current Security Components

Your organization's current security components can be integrated for a centralized view of your mobile exposure, security-related practices, processes, events, and alerts — all presented in an actionable and consolidated dashboard.

To Secure Mobile we must:

1.) SEGMENT

2.) MONITOR

Summary & Availability:

Provides Comprehensive Real-time Cyber Situational Awareness

- Threat Status
- Vulnerability Status
- Compliance Status
- Incident Status
- Risk Status

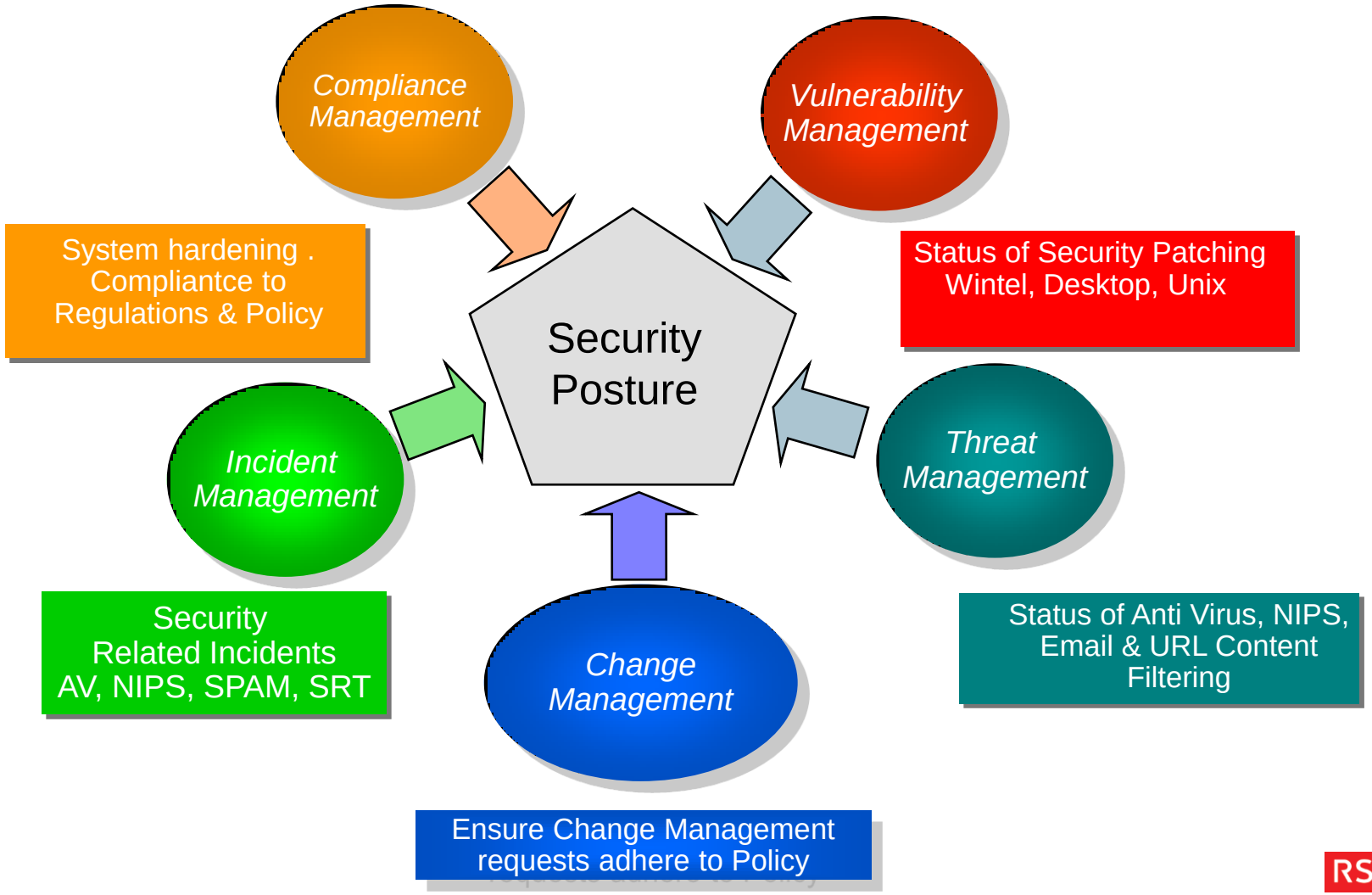
“See Less, Understand More…”

At A Glance

- **Real-time data:** Enterprise dashboard integrates data from existing security controls into one easy-to-understand dashboard view
- **Highly customizable:** Allows you to customize your dashboard for specific job titles and roles
  - Executive Management, CISO, SOC Analysts, Auditors, etc.
- **Drill-down:** Start with a bird's eye view of your data, and drill down to the smallest of details
- **Technology Agnostic:**
  - SIEM (RSA, Symantec, Arcsight etc)
  - Supports a variety of other security controls
- **Perfect for Traditional & Cloud IT:** Works with traditional and CSC Trusted Cloud IT infrastructure
- **Non Intrusive** No infrastructure changes needed

Security Category	Category Score	Target Category Score	Risk Rating - by Category	Category Weighting	Security Score and Risk Rating	Agreed Target
Threat Management	71	75	High	4	67	79
Vulnerability Management	84	75	Medium	3		
Compliance Management	78	60	High	1		
Incident Management	20	100	Extreme	1	High	High
Change Management	40	100	Extreme	1		

Captures “controls based evidence”, security information, events, metric across security domains providing a holistic view of security and risk posture



Thank You

DEAN WEBER
dweber6@csc.com


CSC
BUSINESS SOLUTIONS
TECHNOLOGY
OUTSOURCING