

National Cyber Security Awareness Month

Week Four:

Your Evolving Digital Life

Webinar Recording and Evaluation Survey

- This webinar is being recorded and will be made available online to view later
 - Recording will also be available at www.naco.org/webinars
- After the webinar, you will receive a notice asking you to complete a webinar evaluation survey. Thank you in advance for completing the webinar evaluation survey. Your feedback is important to us.

Tips for viewing this webinar:

- The questions box and buttons are on the right side of the webinar window.
- This box can collapse so that you can better view the presentation. To unhide the box, click the arrows on the top left corner of the panel.
- If you are having technical difficulties, please send us a message via the questions box on your right. Our organizer will reply to you privately and help resolve the issue.

Today's Speakers



Mr. Michael Echols
Chief Information Security
Officer Maricopa County, Ariz.



Dr. Roger Wards
Chief Accountability Officer,
Vice President of Operations
and Planning, Vice Dean of
the Graduate School,
University of Maryland



Steve Hurst,
Director, Security Services and
Technology,
AT&T Inc.



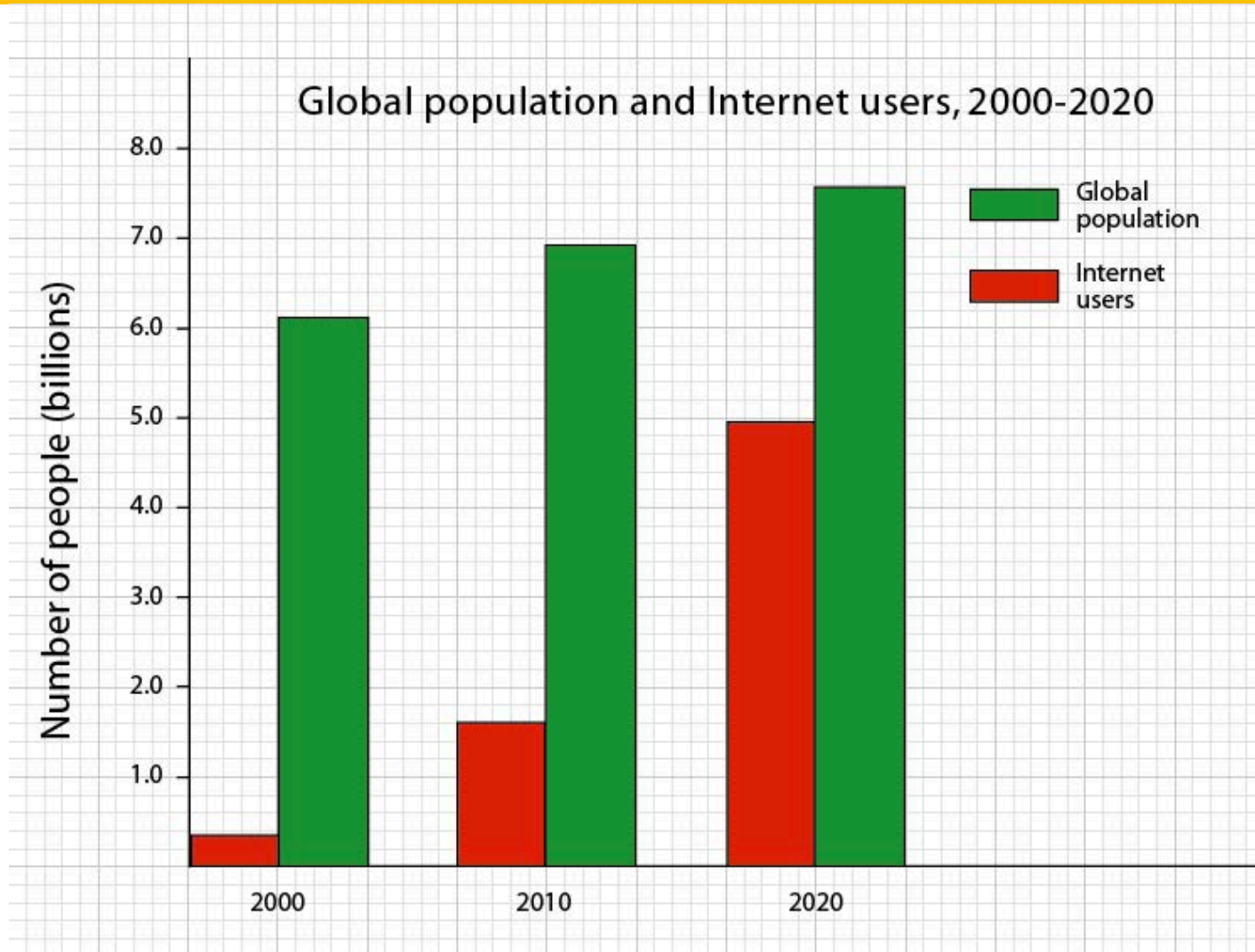
Office of Enterprise Technology

Mobile Trends, Risk and Mitigation

October 21, 2015

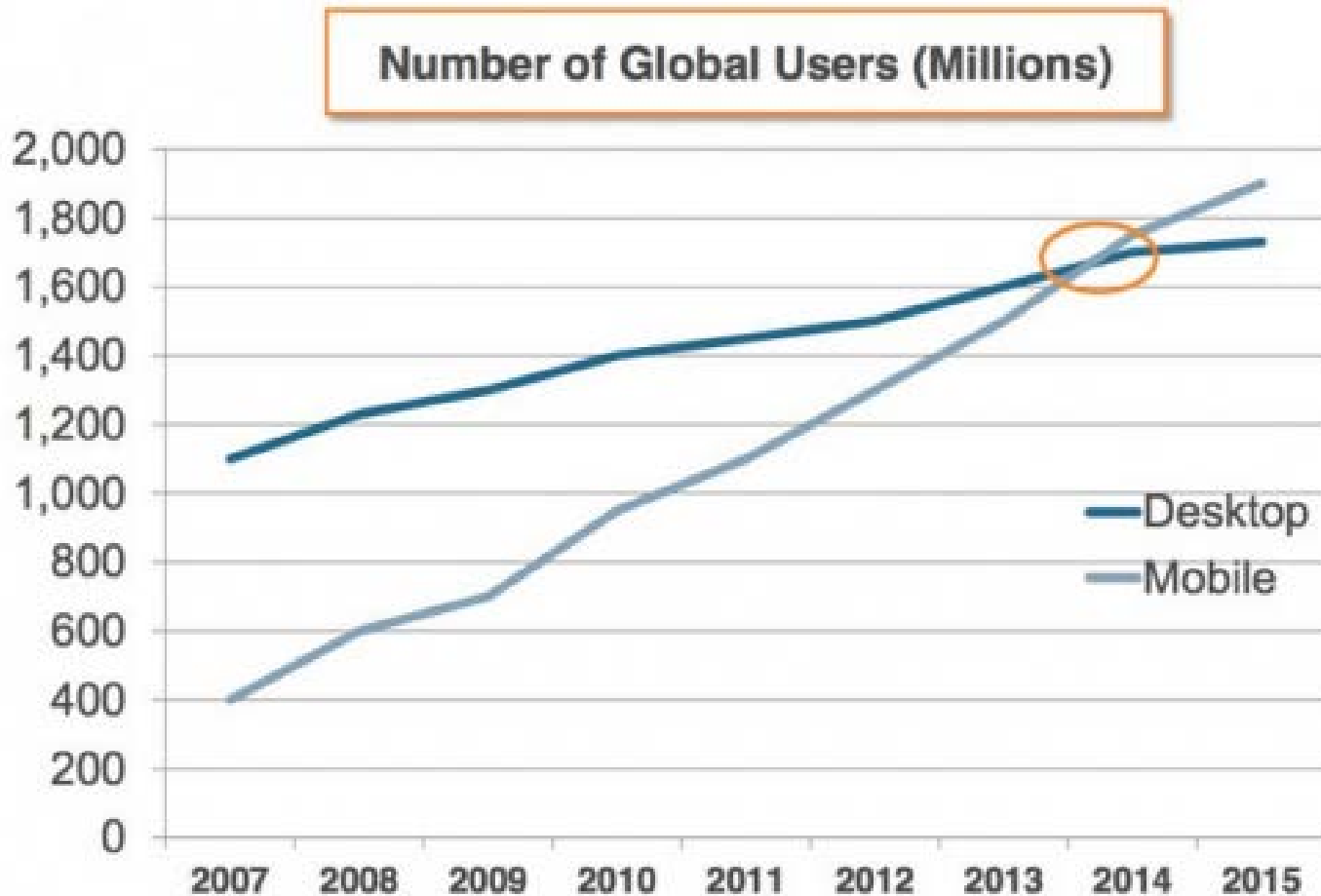
Prepared By
Michael Echols, Chief Information Security Officer

Internet Use Trends







Source: Smart Insights, Mobile Marketing Statistics 2015

Mobile Use Trends



Source: Smart Insights, Mobile Marketing Statistics 2015

IOS and Android Vulnerabilities

VULNERABILITIES UXSS In particular, SSL/TLS misuse and other crypto-related vulnerabilities are common to apps. Attackers are also more often exploiting Universal Cross-Site Scripting (UXSS) vulnerabilities.	ENPUBLIC APPS 1400 These apps bypass Apple's strict review process by hijacking a process normally used to install custom enterprise apps. Many EnPublic apps invoke risky private APIs. In the wrong hands, these APIs threaten user privacy and introduce many vulnerabilities. We found only 1,400 EnPublic apps, a relatively low number. But this poses an intriguing avenue for attackers in the future.	MALWARE   Although uncommon, attackers are looking closely at this attack vector. They're eager to compromise devices that have not been "jailbroken." Attackers have started to use enterprise/ad-hoc provisioning to deliver iOS malware to non-jailbroken devices through trusted USB connections and over-the-air delivery.
MALWARE  We found millions of mobile malware samples—and that number is growing by the week. Ninety-six percent of malware targets Android. KorBanker, which stole users' bank login credentials, is one example.	VULNERABILITIES 5 billion More than five billion downloaded Android apps are vulnerable to remote attacks. One especially risky vulnerability is known as JavaScript-Binding-Over-HTTP (JBOH).	AGGRESSIVE ADWARE 5.61%  Aggressive ad libraries can leak personal data over the network—sometimes in plain text. Burstly is one of the most popular. It's used in more than 300,000 apps, including 5.61 percent of the 500 most-downloaded ones.

Source: Fire Eye, A Comprehensive Mobile Threat Assessment of 7 Million iOS and Android Apps

Mobile Threats

Mobile Threat Definitions



MALWARE

Apps that steal user data, commit financial fraud, and/or negatively impact device performance.

Malware includes threats such as viruses, trojans, worms, spyware, and ransomware.



CHARGEWARE

Apps that charge users for content or services without clear notification or the opportunity to provide informed consent.



ADWARE

Apps that serve obtrusive ads that interfere with standard mobile operating experiences and/or collect excessive personal data that exceeds standard advertising practices.

Source: Lookout Mobile, 2014 Mobile Threat Report

Mobile Malware Examples

ScarePackage | RANSOMWARE

ScarePackage masquerades as an Adobe Flash update or a variety of anti-virus apps, and is distributed as a drive-by-download. When downloaded, it pretends to scan victims' phones and then locks the device after falsely reporting that its scan found illicit content. ScarePackage then displays a fake message from the FBI and attempts to coerce victims into paying them to avoid criminal charges and regain control of their device.⁹

DeathRing | TROJAN

DeathRing poses as a ringtone app and then surreptitiously downloads fake SMS content to infected devices, in a possible attempt to capture victim login credentials by impersonating trusted entities like banks via SMS. Notably, DeathRing appears to come pre-installed on certain devices, suggesting its authors were able to infiltrate the device supply chain and inject their malware into factory-shipped devices.¹⁰

ShrewdCKSpy | SPYWARE

ShrewdCKSpy pretends to be an app marketplace, but the market icon disappears on first launch and the malware starts to run in the background, intercepting and recording victims' SMS and phone calls and uploading them to a remote server. ShrewdCKSpy also has the ability to auto-accept and record calls, which means attackers could possibly turn a victim's phone into a de facto bugging device by auto-accepting their own call.¹²

Source: Lookout Mobile, 2014 Mobile Threat Report

Mobile App Risks

APPS COLLECT YOUR INFORMATION

MOST APPS COLLECT DETAILED INFORMATION ABOUT WHERE YOU GO AND WHAT YOU DO WITH YOUR DEVICE

82%

READ YOUR
DEVICE ID

64%

KNOW YOUR
WIRELESS CARRIER

59%

TRACK LAST
KNOWN LOCATION

55%

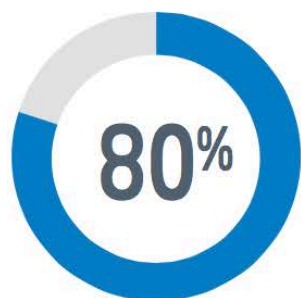
CONTINUOUSLY
TRACK LOCATION

26%

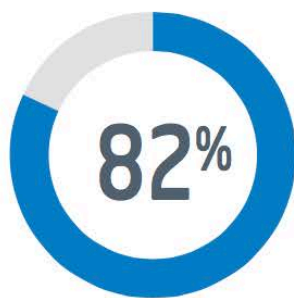
READ THE APPS
YOU USE

26%

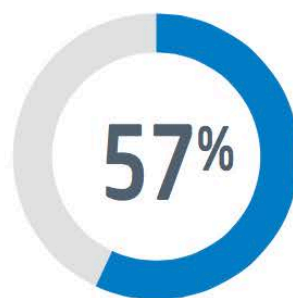
KNOW YOUR SIM
CARD NUMBER



COLLECT LOCATION



TRACK SOMETHING



TRACK WHEN YOU USE
YOUR PHONE

36%

KNOW YOUR ACCOUNT
INFORMATION

Source: McAfee Mobile Security Report February 2014

Actions that will increase safety

1.

Auto-lock your phone

2.

Keep your apps and device software up to date

3.

Use discretion when downloading apps

4.

Stick to window-shopping on public WiFi

5.

Protect your phone like you protect your PC

Your New Connected Life

Steven Hurst CISSP, ISO 27001 Auditor
Director, Security Services & Technology
AT&T, Global Customer Security Services

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. The information contained herein is not an offer, commitment, representation or warranty by AT&T and is subject to change.



Ubiquitous computing



Connected Car



Advancing the Connected Car Reality



Connected Home



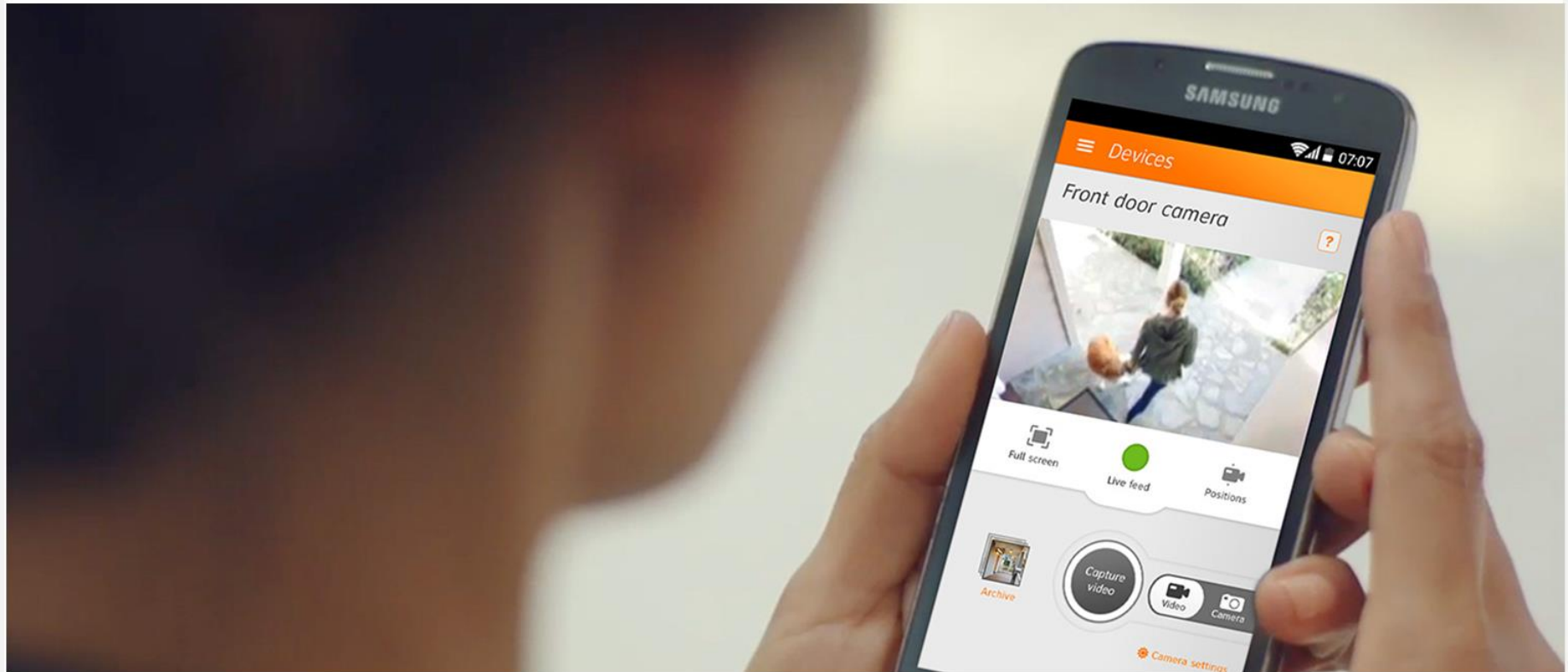
Connected Home



Connected Home



Connected Home



Connected Home



Connected Home



Connected Travel





bellhop.att.io/Login.html#selectLuggage

11:04 AM

0 My Luggage 0

Add +

Live

New York, NY (10:55 am)

Battery Level: 99%



Turn Light On



Back

Modify Luggage

Delete

Serial Number: 004



Live

25" Softside Spinner

Text Notifications

On

Cancel

Save

Report Lost Luggage



AT&T

bellhop.att.io/Login.html#MapTripView

11:04 AM

History

Plano, TX-Plano, TX (5/14/14)
Live

Palo Alto, CA-Palo Alto, CA (3/26/14)
Live

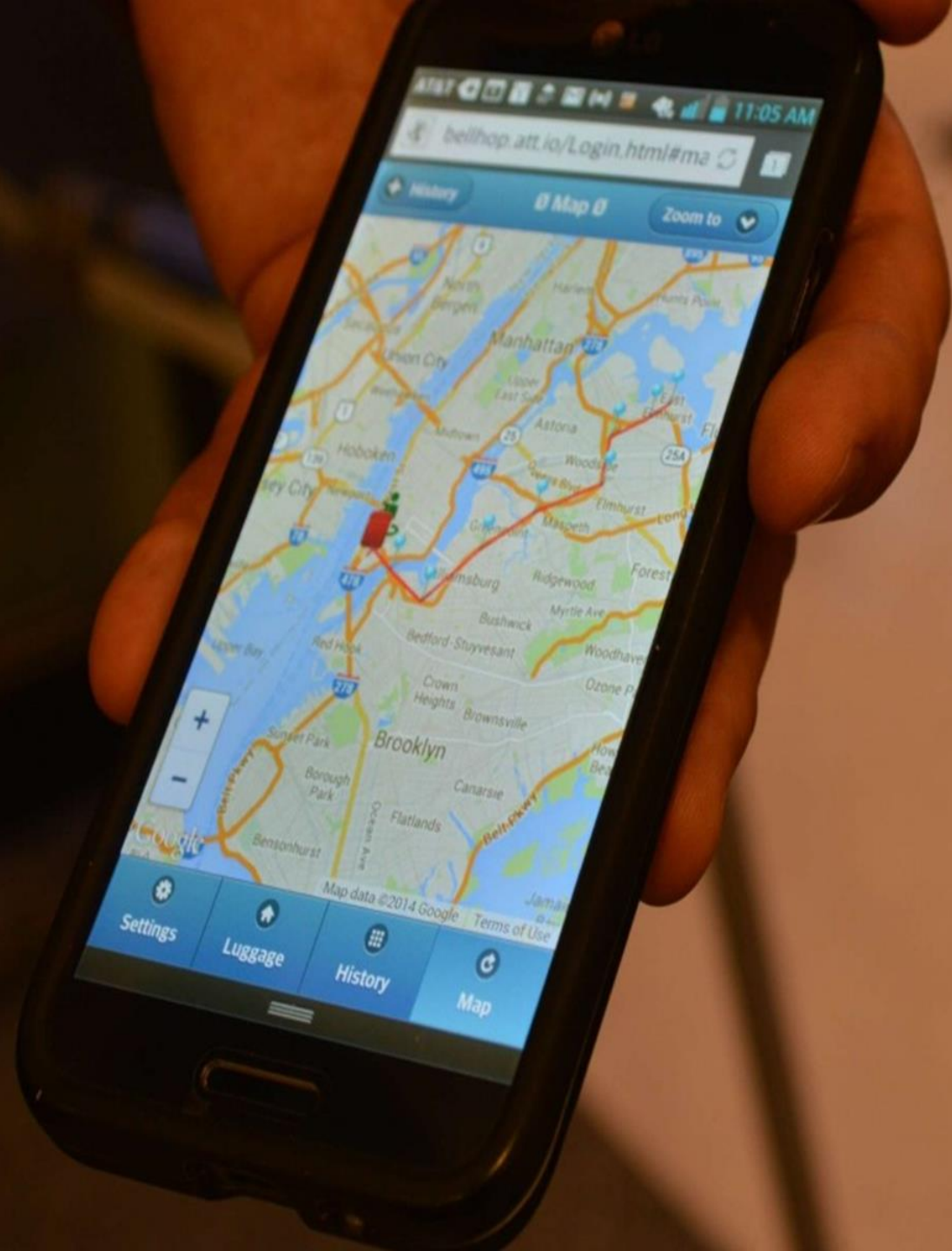
ATL to AT&T Offices (12/19/13)
Live

UPS Hub Rockford, IL (12/19/13)
Live

Foundry to DFW (12/17/13)
Live

Settings

Luggage

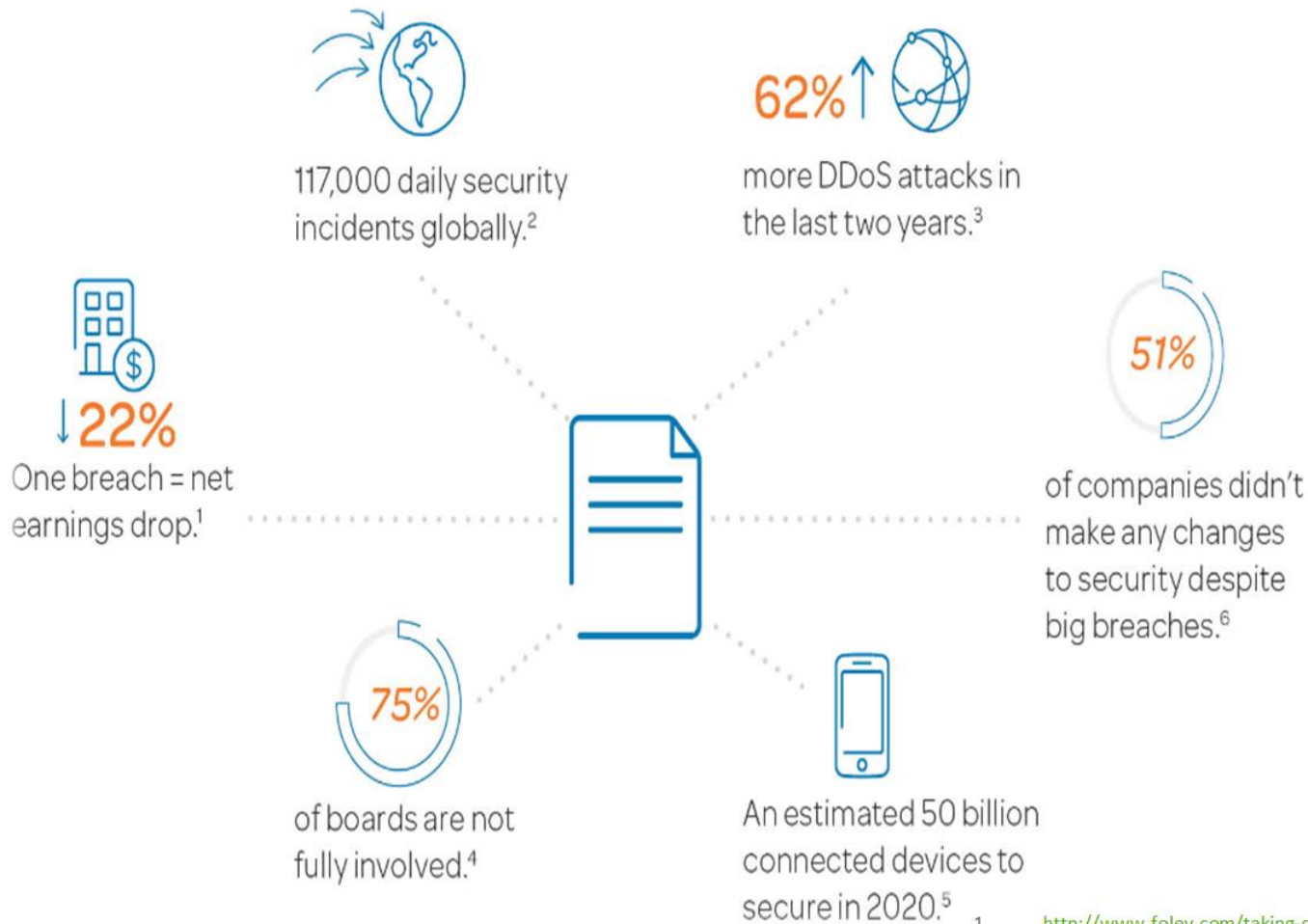




Connected Everything “Back to the Future”



Growth in cyber risks



1. <http://www.foley.com/taking-control-of-cybersecurity-a-practical-guide-for-officers-and-directors-03-11-2015/>
2. PwC Global State of Information Security Survey 2015.
3. AT&T Security Operations Center
4. PwC U.S. State of Cyber Security 2015
5. Cisco, Inc.
6. IDG "State of the CSO" Survey 2015.

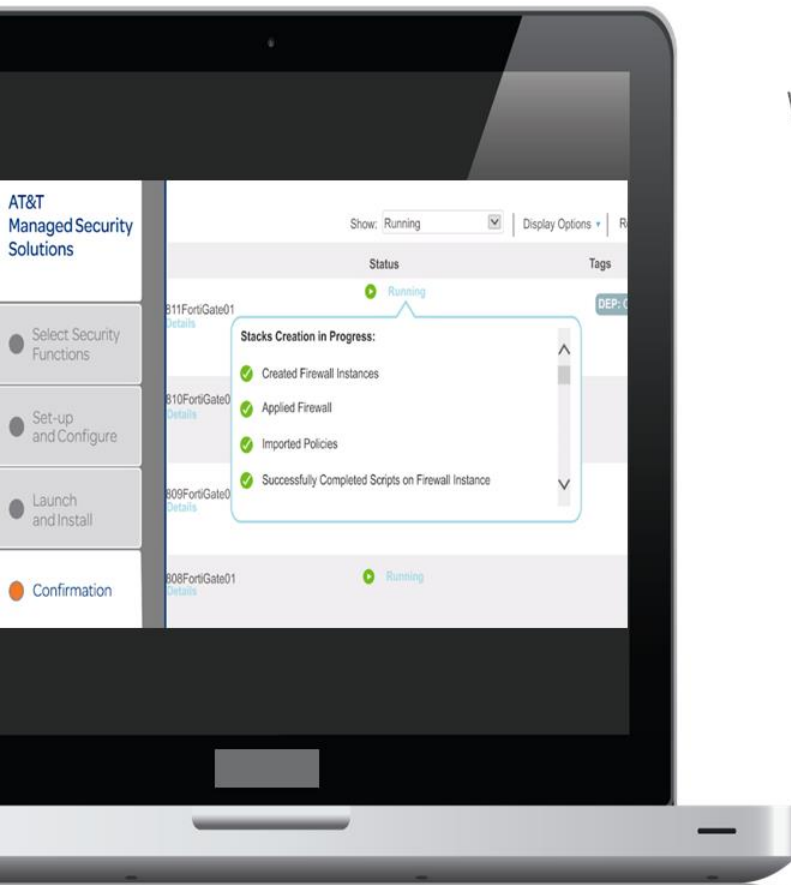


AT&T approach for cyber security

Observe, protect, and prevent



Virtual security managed and deployed where needed



Robust Security Functions

Web Filtering



Intrusion Detection



Firewalls



Data Loss Prevention



Vulnerability Scanning



Deployable to Where You Are



AT&T
Network
Cloud



Private
Cloud



Public
Cloud



CPE/Data
Center



MOBILIZING
YOUR
WORLDSM





UNIVERSITY of MARYLAND

“Your Evolving Digital Life” Implications for higher education

Presenter

Dr. Roger J. Ward

Vice President, Planning and Operations

Vice Dean, Graduate School

Chief Accountability Officer

National Association of Counties Cybersecurity Webinar Series

October 21, 2015

Presentation Overview

- About University of Maryland, Baltimore (UMB)
- Post-traditional Learners and Digital Natives
- Smart World Challenges for Higher Education
- Cyber Risks for Higher Education: Data Breaches
- Managing the Risks

About the University of Maryland, Baltimore (UMB)

- **UMB** is the founding campus (1807) of the University System of Maryland.
- **Mission:** To improve the human condition and serve the public good of Maryland and society at-large through education, research, clinical care and service.
- **Schools:** Dentistry, Graduate, Law, Medicine, Nursing, Pharmacy & Social Work
- **Students:** 6,205
 - Graduate and Professional: 87%
 - Undergraduate: 13%
 - Full-time: 77%; Part-time: 23%
- **Employees** (includes faculty): 7,858;
 - Full-time: 71%; Part-time: 29%
 - Faculty: 1,908(full-time); 943(part-time)
- **Annual Budget:** ~\$1B
- **Grants and Contracts:** ~\$500k

Drivers of Change: Rise of the Post-Traditional Learner

- Traditional learners are students that go to college immediately after high school, attend full-time, and are financially dependent on their parents. They attend four-year colleges and live on campus.
- Over the last 30 years, however, the data indicate that the number of students actually fitting this traditional model has been dropping.
- The startling reality is that, according to the National Center for Education Statistics, today traditional students represent only about 15 percent of current undergraduates.
- The remaining 85 percent of undergraduates are a diverse group that includes adult learners, employees who study, low-income students, commuters, and student parents.

Drivers of Change: Rise of the Post-Traditional Learner

- Post-traditional learners are working-age (25 to 64 years) students who demand “customized education” integrating their professional experience with tailored learning.
- Post-traditional learners tend to already be a part of the workforce and seek the flexibility of online learning to acquire new skills necessary for advancement in their current professions.
- The demand for online learning is driven in large measure by the rise of the post-traditional learner.
- Approximately, 51% of post-traditional learners are seeking certificate or a technical/occupational license, with the bulk of the remainder interested in professional masters degrees.

Digital Natives

- The term 'digital native' refers to students born after 1980 when the personal computer became commonplace.
- Technology had created a discontinuity, resulting in a radical change in the characteristics of the new generation of students entering our universities.
- They are the most technologically networked generation in history.

Students Use of Technology

- Outside of school:
 - Email, Internet, social media, texting on cell phones, instant messaging, and talking on cell phones.
- In school
 - Accessing information on the Internet, using email, word processing, math and science programs, texting on cell phones, and accessing electronic databases.

Students' Use of Technology: Trends

- Students expect to be able to work, learn, and study whenever and wherever they want to.
- Life in an increasingly busy world where learners must balance demands from home, work, school, and family poses a host of logistical challenges with which today's ever more mobile students must cope.

(NMC Horizon Report, 2012)

Smart World Challenges for Higher Education

- The abundance of resources made easily accessible via the Internet is increasingly challenging us to revisit our roles as educators.
- Universities have always been seen as the gold standard for educational credentialing, but emerging certification programs from other sources are eroding the value of that mission daily.
- The technologies we use are increasingly cloud-based.
- It does not matter where our information is stored; what matters is that our information is accessible no matter where students are or what device they choose to use.

Smart World Challenges for Higher Education

- Education paradigms are shifting to include online learning, hybrid learning and collaborative models.
- Institutions that embrace face-to-face/online hybrid learning models have the potential to leverage the online skills learners have already developed independent of academia.

(NMC Horizon Report, 2012)

Smart World Challenges for Higher Education

- Digital media literacy continues its rise in importance as a key skill in every discipline and profession.
- Despite the widespread agreement on the importance of digital media literacy, training in the supporting skills and techniques is rare in teacher education and non-existent in the preparation of most university faculty.

(NMC Horizon Report, 2012)

Data breaches in a Digital Higher Education Environment

- As of April 25, 2014, the Privacy Rights Clearinghouse (PRC) documented 4,257 data breaches in the US involving at least 867,217,832 records from all industry sectors.
- Education has a larger number of reported breaches but fewer records exposed.
- 63% of the PRC reported breaches are attributed to doctoral institutions, though they make up only 7% of all U.S. institutions.
- 21% of the reported breaches are attributed to master's (MA) institutions, which make up 16% of all U.S. institutions.
- While they comprise the majority of U.S. higher education institutions, associate's (AA) and bachelor's (BA) institutions had fewer reported data breaches.

Data breaches in higher education: Top 5 categories

1. **Hacking or malware:** Electronic entry by an outside party; data loss via malware and spyware.
2. **Unintended disclosure:** Sensitive information posted publicly on a website, mishandled, or sent to the wrong party via e-mail, fax, or mail.
3. **Portable device:** Lost, discarded, or stolen portable devices (e.g., laptop, PDA, smartphone, portable memory device, CD, hard drive, data tape, etc.).
4. **Stationary device:** Lost, discarded, or stolen stationary electronic device such as a computer or server not designed for mobility.
5. **Physical loss:** Lost, discarded, or stolen non-electronic records, such as paper documents.

ERM as a framework for managing cyber risk

- It is a process initiated and effected by an organization's leadership;
- Developed and managed at the 'enterprise' as opposed to the unit or operational level;
- Designed to identify and mitigate risks that would impact strategic objectives; and
- Provides a framework for determining risk tolerance, developing mitigating strategies, and allocating resources.



UNIVERSITY *of* MARYLAND

The End

Q&A



You may ask a question using the questions box on the right side of the webinar window.

Contact Information

Jerryl Guy, MS, MCSE, CISSP

IT Manager, NACo

Email: jguy@naco.org

Phone: (202) 942-4229