

# Identity Management: Are You Really a Dog Surfing on the Internet?



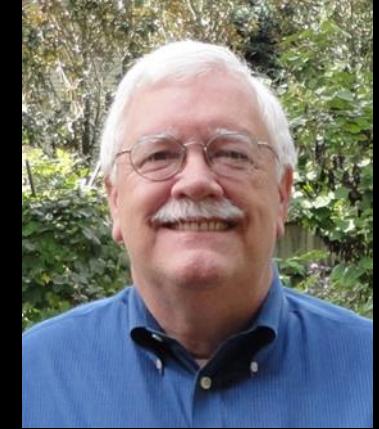
**June 25, 2013**

Start Time: 9 AM US Pacific,  
Noon US Eastern, 5 pm London

**Generously sponsored by:**



# Welcome Conference Moderator



**Phillip H. Griffin**

*ISSA Fellow, Raleigh, USA Chapter*

*ISSA Web Conference  
Committee*



# Agenda

## Speakers

- **Malcolm Harkins**

*Vice President, Software and Services Group, Chief Security and Privacy Officer, Intel Corporation*

- **Nathan Moon**

*IT Security Architect/Administrator at Intermountain Health Care*

- **Jaimon Jose**

*Distinguished Engineer, Office of the CTO, NetIQ*

## Open Panel with Audience Q&A

## Closing Remarks

# ISSA Identity Webinar



**Malcolm Harkins**

*Vice President,  
Software and Services Group,  
Chief Security and Privacy  
Officer, Intel Corporation*



# ISSA Identity Webinar

**Malcolm Harkins**

Vice President  
Chief Security and Privacy Officer



# Legal Notices

This presentation is for informational purposes only. INTEL MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY.

BunnyPeople, Celeron, Celeron Inside, Centrino, Centrino Inside, Core Inside, i960, Intel, the Intel logo, Intel AppUp, Intel Atom, Intel Atom Inside, Intel Core, Intel Inside, the Intel Inside logo, Intel NetBurst, Intel NetMerge, Intel NetStructure, Intel SingleDriver, Intel SpeedStep, Intel Sponsors of Tomorrow., the Intel Sponsors of Tomorrow. logo, Intel StrataFlash, Intel Viiv, Intel vPro, Intel XScale, InTru, the InTru logo, InTru soundmark, Itanium, Itanium Inside, MCS, MMX, Moblin, Pentium, Pentium Inside, skoool, the skoool logo, Sound Mark, The Journey Inside, vPro Inside, VTune, Xeon, and Xeon Inside are trademarks of Intel Corporation in the U.S. and other countries.

\*Other names and brands may be claimed as the property of others.

Copyright © 2011, Intel Corporation. All rights reserved.



**Intel Security and Privacy Office**  
Protecting to Enable People, Data & Business



# Building a Trust Model

***Decide the access level*** you want to give employees based on your security resources

***Decide if you need to segment your users*** and provide a higher access levels for certain users

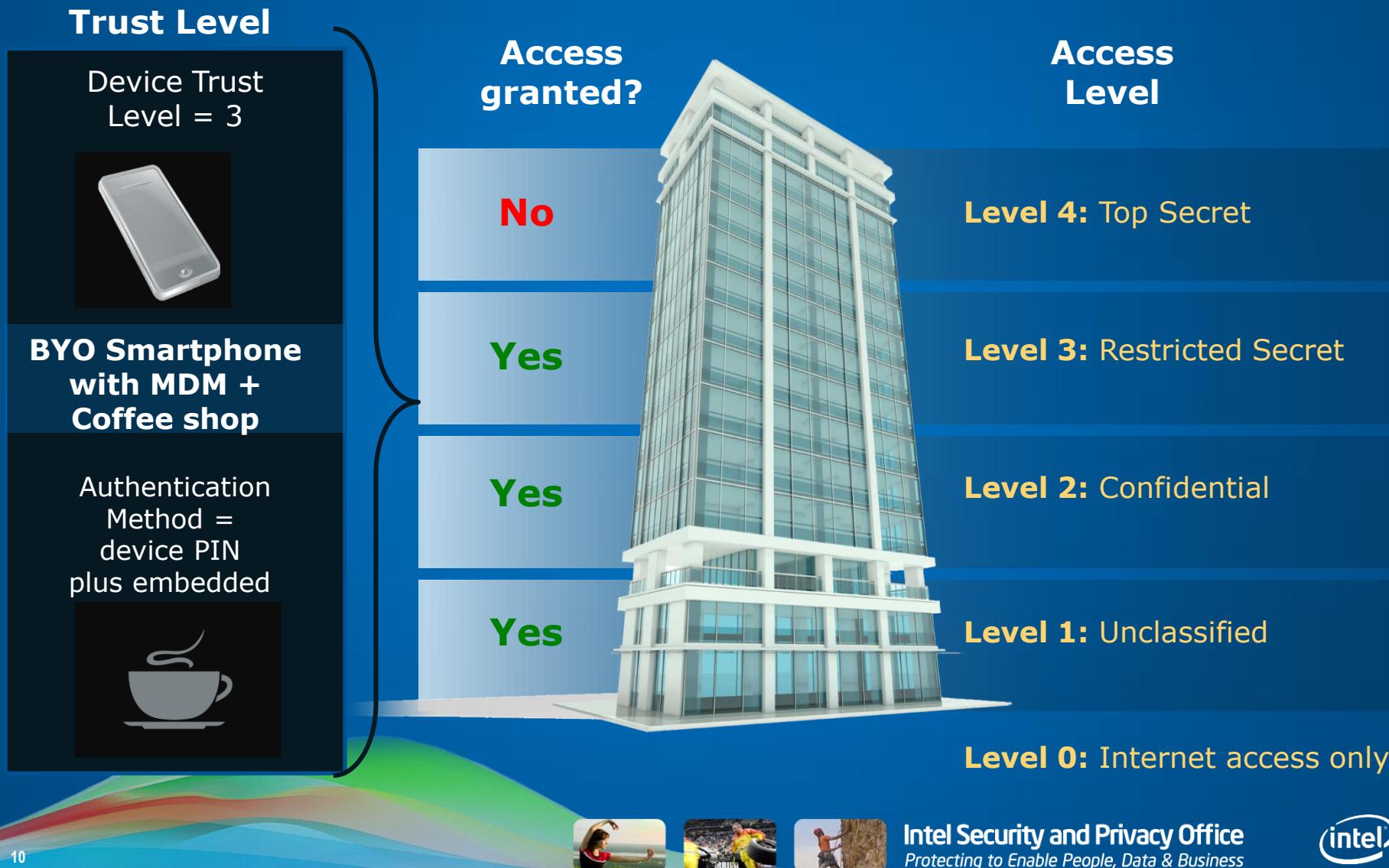
***Dial up your detective/monitoring controls*** and build up your preventive controls over time



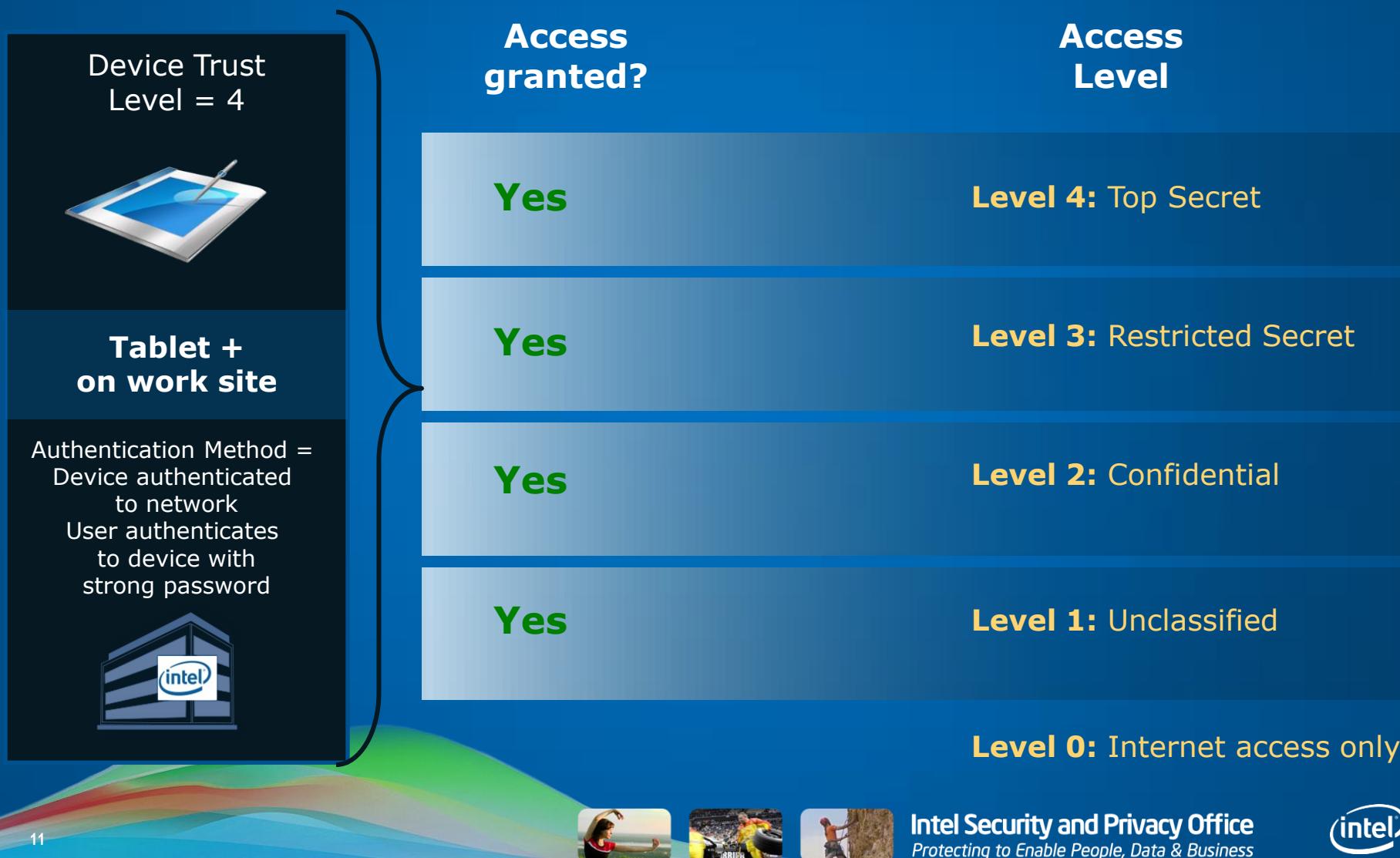
**Scenario A:** BYO smartphone with no MDM, but has OTP with PIN.  
User will have a lower access level and minimum information.



**Scenario B:** Employee has a BYO smartphone with OTP, MDM, and current version of OS. User access increases and more information flows.



**Scenario C:** Employee has a BYO tablet with MDM plus anti-virus, intrusion detection, firewall, and centralized logging. User has highest access level with access to most sensitive data.



# Look Ahead

Pick your agreement  
Who else (other then you) can use your phone?



Only me

My family

Family & friends



# Device Proximity: Better Access Rules



**Intel Security and Privacy Office**  
Protecting to Enable People, Data & Business



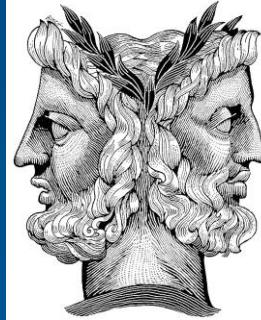
# User's Identity Data is Being Shared



Once Lost, Private Data Cannot be Reclaimed!



# Multiple Personalities and Identity



**How do we evolve our products to address the 'Janus' issue with Identity solutions today?**

- One persona on multiple devices
  - Personal cloud/Device Constellation
- Multiple Personas for a single user on their Device(s)
  - A work persona and a personal persona
- Multiple Personas (different users) on the same Device (known users)
  - A family shared device, ex. Tablets, TV, Game Console
- Multiple Personas (different users) on the same Device (unknown users)
  - Internet Kiosk, Rental Car, Gaming Cafe
- A single account used by multiple personas on the same device (account binding issue)
  - Shared Content Streaming, ex. Netflix



# Persona & Multi-Tenancy Requirements

- The Internet is becoming a distributed virtual network that is both collaborative AND private.
- Personas need to exist across multiple devices and services and users can wear multiple hats
  - Work, home, volunteer, parent, club, gym, consumer etc...)
- Potentially every device and service must enforce multi-tenant isolation AND link to other personas collaboratively engaged
- Other collaborators need assurance that a real and authorized person is behind the persona



# Thank You



# Question and Answer

Malcolm Harkins

*Vice President,  
Software and Services Group,  
Chief Security and Privacy  
Officer, Intel Corporation*



# Identity Management: Evolving Issues and Strategies in Healthcare



**Nathan Moon**  
*Utah, USA Chapter*

*IT Security Architect/  
Administrator  
Intermountain Health Care*

# About the Speaker

- I.S. Security Architect for Intermountain Healthcare
- 17 years of security experience in developing security solutions for the healthcare environment
- 11+ years in developing and implementing Identity and Access Management solutions

# About Intermountain Healthcare

- Intermountain Healthcare  
[\(http://www.intermountainhealthcare.org\)](http://www.intermountainhealthcare.org)
  - An internationally recognized, nonprofit integrated healthcare system with 33,000 employees
  - 22 hospitals
  - A Medical Group with more than 185 physician clinics
  - An affiliated health insurance company
  - Surgery and outpatient treatment centers
  - Multi-specialty clinics including physician offices, InstaCare, KidsCare, Homecare, Hospice, Lab Services, and WorkMed occupational health clinics

# Identity – User Management Concepts

- Identifies who we are and what we can do
  - Important for the individual
  - Critical for businesses wanting: central component of security strategy
- Identities change when concept is added or updated
- Our identities are found in many different ‘user stores’ or ‘directories’
  - Online vs. Private
- Is this old news?

# Identity Challenges 10 Years Ago



- We struggled with:
  - Inconsistency in user management
  - Poor tracking of user access
  - User frustration to gain access
  - Minimal vendor support
- Has the problem been resolved today?

# Maybe?

- Improved vendor support for open user standards
- Improved identity and password management systems
- Enhanced integration with federation services
- Improved workflow between HR systems and identity systems
- However.....

# Still Have Existing Challenges

- Vendors are still slow to adopt open authentication and authorization standards
  - Usage of LDAP is still not globally adopted for authentication
  - Majority of applications still require disparate user directories to control/maintain for authorization purposes
- Web SSO and Enterprise SSO space do not have open standards; man vended solutions are still proprietary
- Number of applications continue to increase without adopting open standards
- Landscape continues to evolve
- PKI

# Evolving Landscape

- Cloud applications
- Increase demand for off-site resources (including off-shore resources)
- Expanding networks
- Health Information Exchanges (HIE)

# What does the future hold?

- Continue with current struggles as vendors work to support open standards
  - LDAP
  - SAML
  - XACML
- Health Information Exchanges
  - Identity source
  - Opt in / Opt out
- Expansion of Patient Portals and Technologies
  - Linking of ‘identity directories’ (Facebook, Google+, etc.)
  - TeleHealth
- Migration from ‘password token’ technologies

# Question and Answer

Nathan Moon  
*Utah, USA Chapter*

*IT Security Architect/  
Administrator  
Intermountain Health Care*



# BYOI: Passport to Future IT



Jaimon Jose

*Distinguished Engineer  
Office of the CTO, NetIQ*



# Evolution of Identity



Personal identity is the unique numerical identity of persons through time<sup>1</sup>

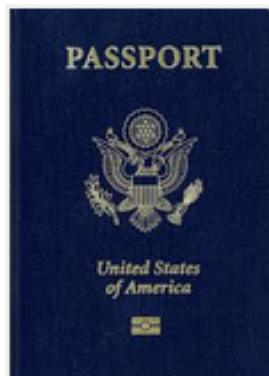
Resolved Question

Show me another »

Is it weird to make a Facebook account for a newborn baby and for parents to post as the baby?



Electronic and physical identities are converging

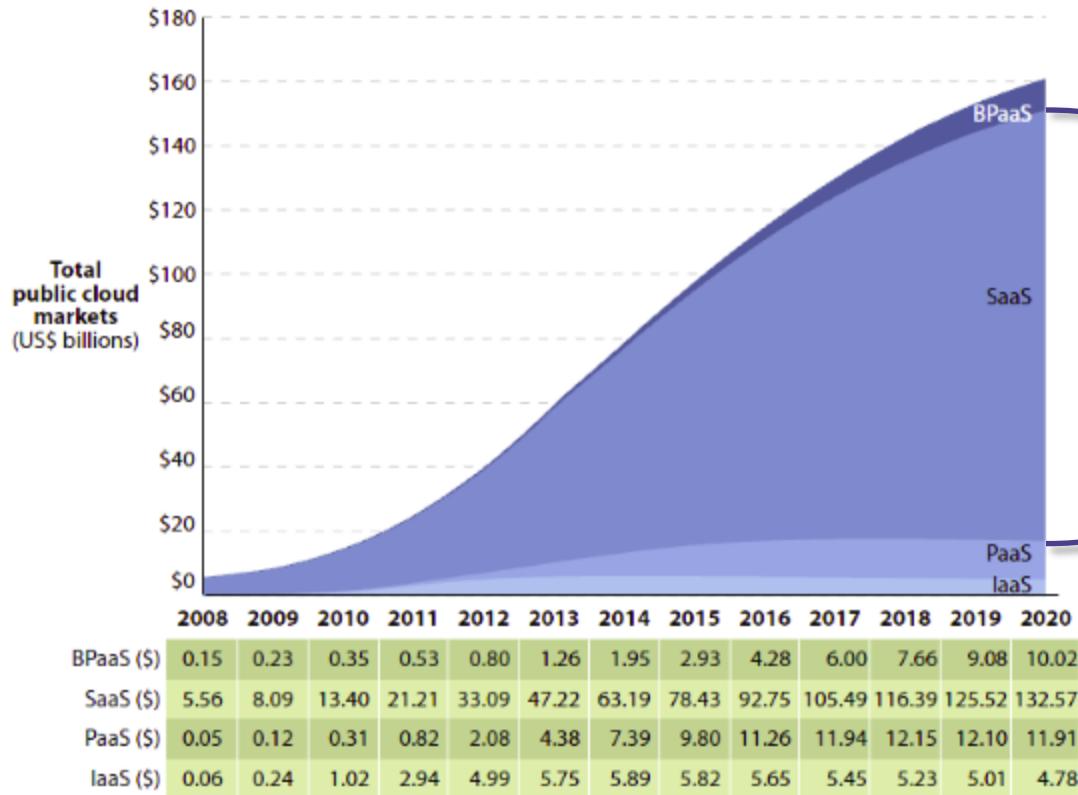


What does it take for individuals to persist from moment to moment—or in other words, for the same individual to exist at different moments?

# Growing SaaS Market Opportunity

Figure 3 Forecast: Global Public Cloud Market Size, 2011 To 2020

The spreadsheet detailing this forecast is available online.



58161

Source: Forrester Research, Inc.

- The total global SaaS market size is projected to grow to **\$132.5 billion in 2020.**
- This growth will force more and more organizations to adopt BYOD and BYOI

# BYOD

"The rise of "bring your own device" programs is the single most radical shift in the economics of client computing for business since PCs invaded the workplace...IT's best strategy to deal with the rise of BYOD is to address it with a combination of policy, software, infrastructure controls and education in the near term, and with application management and appropriate cloud services in the longer term."

*(Bring Your Own Device: New Opportunities, New Challenges,  
16 August 2012, Gartner Analyst – David A. Willis)*



# Bring Your Own Device (BYOD)



## Mobile is changing business

- Support for internal and BYOD initiatives
- How is BYOD used within the organization?

The screenshot shows the official website of the White House Digital Government. At the top, it features the text "the WHITE HOUSE PRESIDENT BARACK OBAMA" and the seal of the White House. Below the header, there is a navigation bar with links for "BLOG", "PHOTOS & VIDEO", "BRIEFING ROOM", "ISSUES", and "the ADMINISTRATION". A blue banner across the middle of the page reads "Home • Bring Your Own Device". On the left side of this banner is the seal of the President of the United States. To the right, the words "DIGITAL GOVERNMENT" are prominently displayed. At the bottom of the banner, there are four links: "About the Strategy", "Strategy Milestones", "Deliverables", and "Advisory Group".

## Bring Your Own Device

*A Toolkit to Support Federal Agencies Implementing Bring Your Own Device (BYOD) Programs*  
August 23, 2012

Product of the Digital Services Advisory Group and Federal Chief Information Officers Council

# Bring Your Own Identity (BYOI)



Social networks and BYOI are here

- Business and government want to connect externally
  - How does the business use Social networks?
- Consumers don't like registration screens
  - Social login as an alternative to registration form

A screenshot of the NYC.ID login page. The main area has an orange background with the NYC.ID logo at the top. It features two input fields for 'Username' and 'Password', and a 'Login' button below them. To the right, there is a sidebar with the heading 'Or login using one of these social media sites:' followed by buttons for Facebook, Google, LinkedIn, Windows Live, Twitter, and Yahoo! A small checkmark icon is visible near the bottom of the sidebar.

STAMFORD, Conn., February 5, 2013

[View All Press Re](#)

Gartner Says Half of New Retail Customer Identities Will Be Based on Social Network Identities by 2015

# The Personal/Social Global Identity

→ Personal/Social identity is global

→ Users

- Threat of losing your identity – Identity theft/fraud
- Careless use of social identity – public profile

But he that filches from me my good name  
Robs me of that which not enriches him  
And makes me poor indeed.

- Shakespeare, Othello, act iii. Sc. 3

→ Organizations/merchants

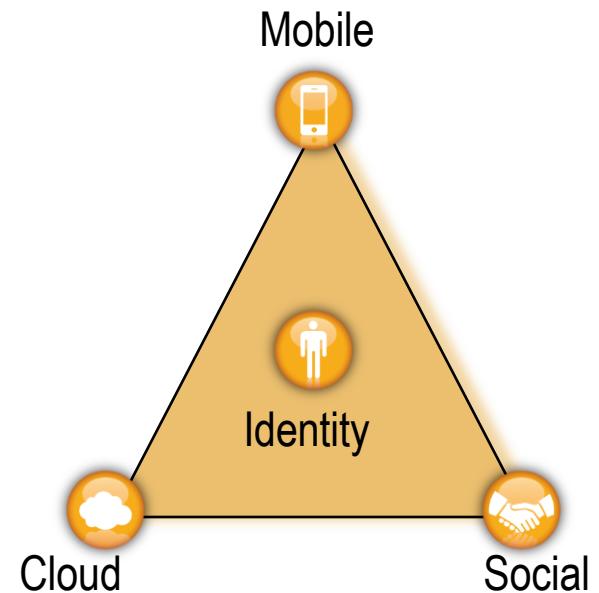
- Possibility of getting exposed to more fraud due to lack of identity proofing and weak authentication of social network identities

# Security Challenges

- Inversion of enterprise IT from an application-centric to a people centric structure

— Peter

Christy, Internet Research Group



The shift to the cloud and the consumerization of IT have complicated the task of identity and access management in the enterprise security environment  
- Mark Diodati, VP, Gartner

- How do you provision accounts?
- Who has access to what?
- Multiple passwords

# Security Challenges

- De-perimeterization of IT
- BYOD brings new risks and values
  - The organization can not take control of the device
  - Its not just Bring Your Own Device, But
    - Bring Your Own Data
    - Bring Your Own Keys and Credentials
    - Bring Your Own Applications
    - Bring Your Own Contacts, Mail and other
- Legacy applications may not be mobile ready

# High-Level Threats and Vulnerabilities<sup>2</sup>

- Lack of physical security controls
- Use of untrusted mobile devices
- Use of untrusted networks
- Use of applications created by unknown parties
- Interaction with other systems
- Use of untrusted content
- Use of location services

2. Guidelines for Managing and Securing Mobile Devices in the Enterprise – NIST, July 2012

# Organizations Should...

- Get ready now, because BYOI/D is coming
- Integrate – You will need to
- Identity runs both ways, so manage cloud access
- Layer your authentication
- Pilot, test and learn

# Choose Your Identity Management Solutions

- Should leverage existing business processes
- Automated provisioning
  - More importantly De-provisioning
- Identity mapping where needed
- Delegated administration
- Simplified and centralized entitlement management
- Quick time to value

# Choose Your Cloud Access Solutions

- Secure access to cloud based applications
  - Single sign-on
  - Automated zero day start/stop
  - Use your familiar administrative console for managing access
  - Use multi-factor/step up authentication for critical resource access
- Integration
  - Use of standard technologies for easier integration
    - SCIM, SAML, OpenID, OpenID Connect, WS-\*, SSL/TLS
    - Business via API
- Consider Mobile Application Management (MAM)

# Question and Answer

Jaimon Jose

*Distinguished Engineer  
Office of the CTO, NetIQ*



# Open Panel with Audience Q&A

- **Malcolm Harkins**

*Vice President, Software and Services Group, Chief Security and Privacy Officer, Intel Corporation*

- **Nathan Moon**

*IT Security Architect/Administrator, Intermountain Health Care*

- **Jaimon Jose**

*Distinguished Engineer, Office of the CTO, NetIQ*

# Closing Remarks

Thank you to our Sponsor



Thank you to Citrix for donating this Webcast service



# CPE Credit

- Within **24 hours of the conclusion** of this webcast, you will receive a link via email to a post Web Conference quiz.
- After the successful completion of the quiz you will be given an opportunity to **PRINT** a certificate of attendance to use for the submission of CPE credits.