



Virginia Information Technologies Agency

Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

February 4, 2015



ISOAG February 4, 2015 Agenda

- | | |
|----------------------------------|---------------------------------------|
| I. Welcome & Opening Remarks | Mike Watson, VITA |
| II. Identity & Access Management | John Ted Childs, IBM |
| III. Shape Up The Scene | Ed Miller, VITA |
| IV. Upcoming Events | Bob Baskette/Michael Watson, VITA |
| V. Partner/Operation Update | Bob Baskette, VITA, Michael Clark, NG |



Welcome and Opening Remarks

Michael Watson

February 4, 2015



John Ted Childs, IBM,
“Identity & Access Management”

February 4, 2015

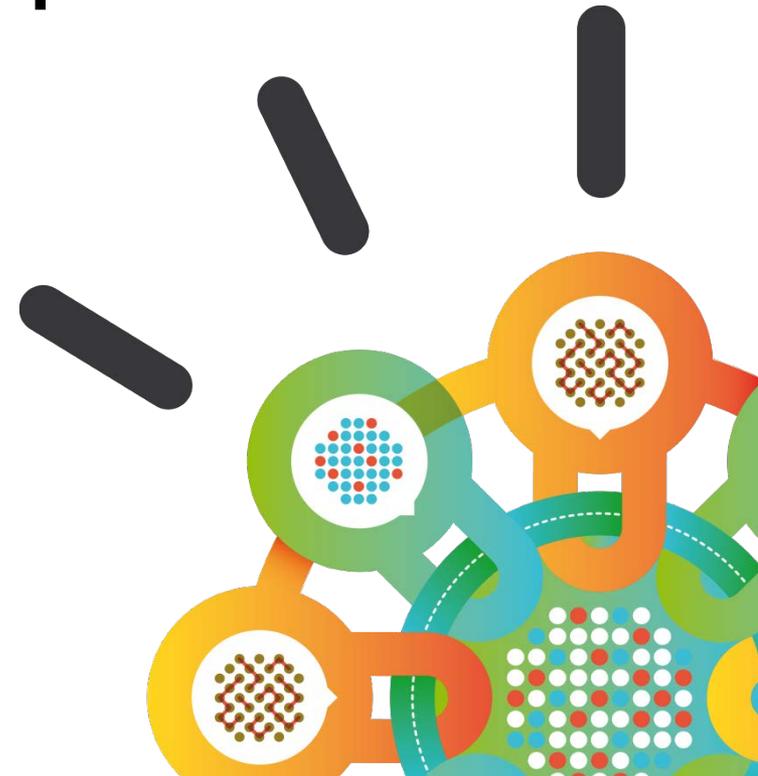
Security Intelligence.
Think Integrated.

IBM Threat-Aware Identity and Access Management for the Open Enterprise

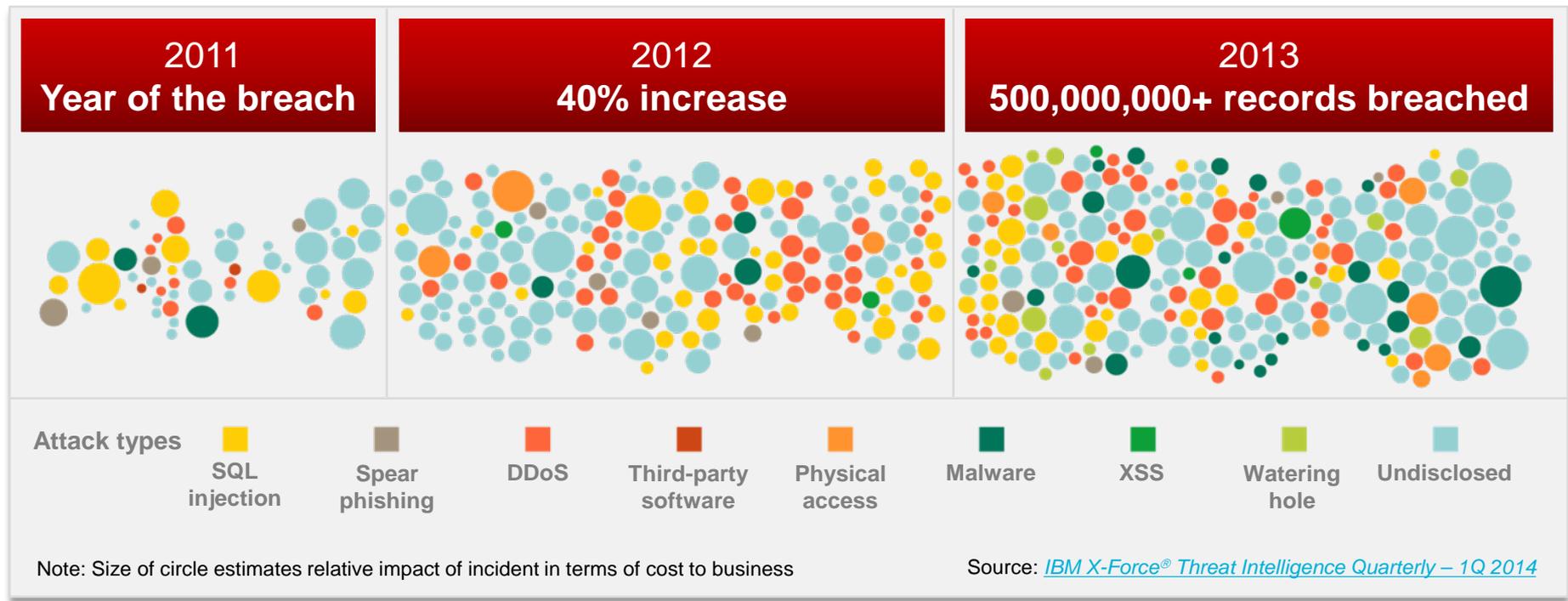
J. Ted Childs, III

BUE NA Identity and Access Sales

January 2015



Sophisticated attackers break through safeguards every day



61% of organizations say data theft and cybercrime are their greatest threats

2012 IBM Global Reputational Risk & IT Study

\$3.5M+ average cost of a data breach

2014 Cost of Data Breach, Ponemon Institute

With vulnerabilities designed to gain unauthorized access

Consequences of exploitation 2013

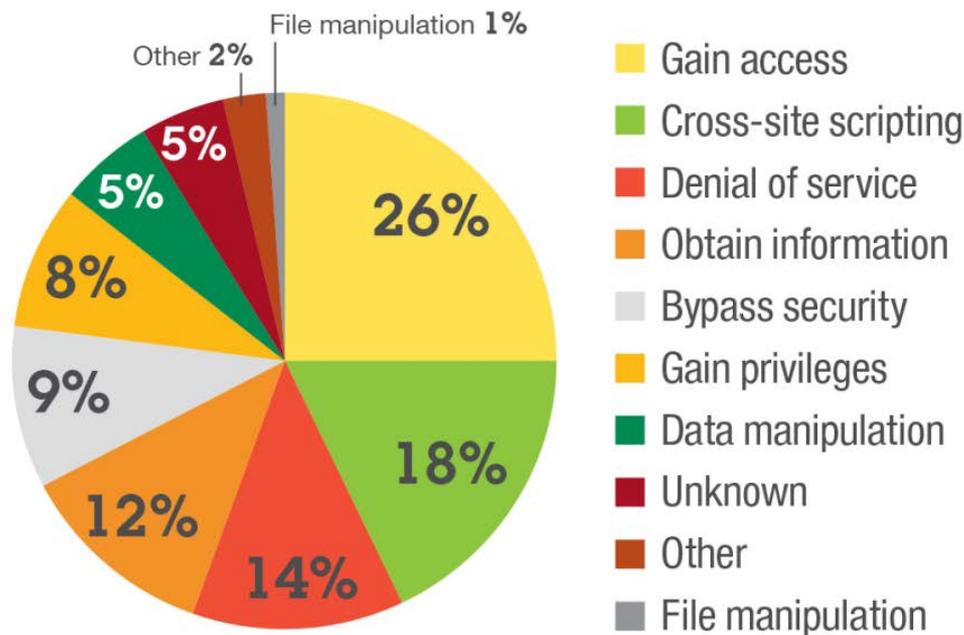


Figure 12. Consequences of exploitation 2013

Source: IBM X-Force® Research and Development

Exploitation

- Gain access
- XSS typically attacks web apps

Consequence	Definition
Gain access	Obtaining local and remote access to an application or system; also includes vulnerabilities by which attackers can execute code or commands, because these usually allow attackers to gain access to the underlying service or system OS
Cross-site scripting	Varying impact depending on the targeted application or user, but could include such consequences as sensitive information disclosure, session hijacking, spoofing, site redirection or website defacement
Denial of service	Crashing or disrupting a service or system
Obtain information	Obtaining information such as file and path names, source code, passwords, or server configuration details
Bypass security	Circumventing security restrictions such as authentication, firewall or proxy, and intrusion detection system (IDS)/intrusion prevention system (IPS) or virus scanners
Gain privileges	Obtaining elevated privileges on an application or system via valid credentials
Data manipulation	Manipulating data used or stored by the host associated with the service or application
Unknown	The consequence cannot be determined based on insufficient information
Other	Refers to anything not covered by the other categories
File manipulation	Creating, deleting, reading, modifying or overwriting files

Table 1. Definitions for vulnerability consequences

Source: IBM X-Force® Research and Development

Security priority focus on Digital Identities as a weak link – People

55% of scam and phishing incidents are campaigns enticing users to click on malicious links

Social media is fertile ground for pre-attack intelligence gathering

Criminals are selling stolen or fabricated accounts



Mobile and Cloud momentum continues to break down the traditional perimeter and forces us to look at security differently

Threat-aware Identity and Access Management become the key line of defense of the open enterprise

The adoption of cloud, analytics, mobile, and social computing is forcing organizations to open IT assets to new business channels



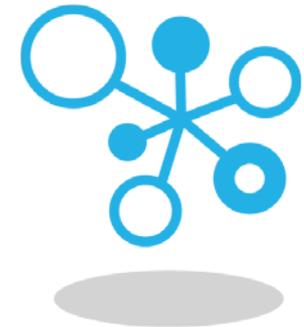
73% of organizations discovered cloud usage outside of IT or security policies



Between 2005 and 2020, the amount of data in the world will grow 300X, from 130 to 40,000 exabytes.



81% of adults use personally owned mobile devices for conducting business



70% of employees are engaged in social activities both internally and externally

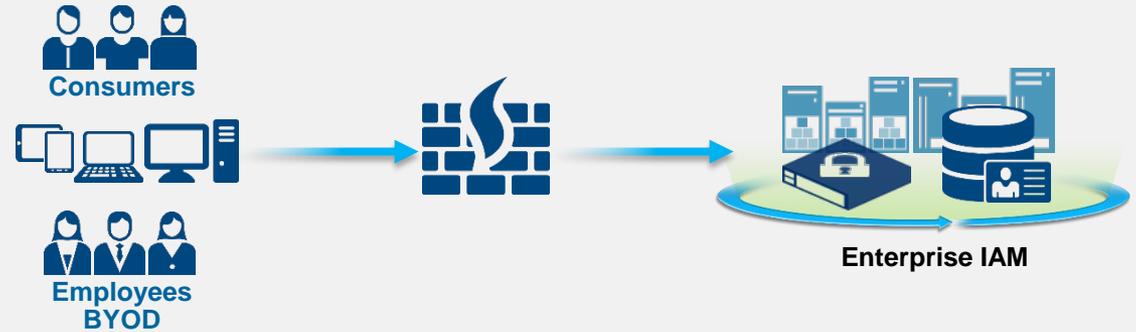
...and challenging them to rethink the way they have traditionally approached security

Digital Identities become a security control for an open enterprise

Traditional IAM

- Operational management
- Compliance driven
- Static, trust-based

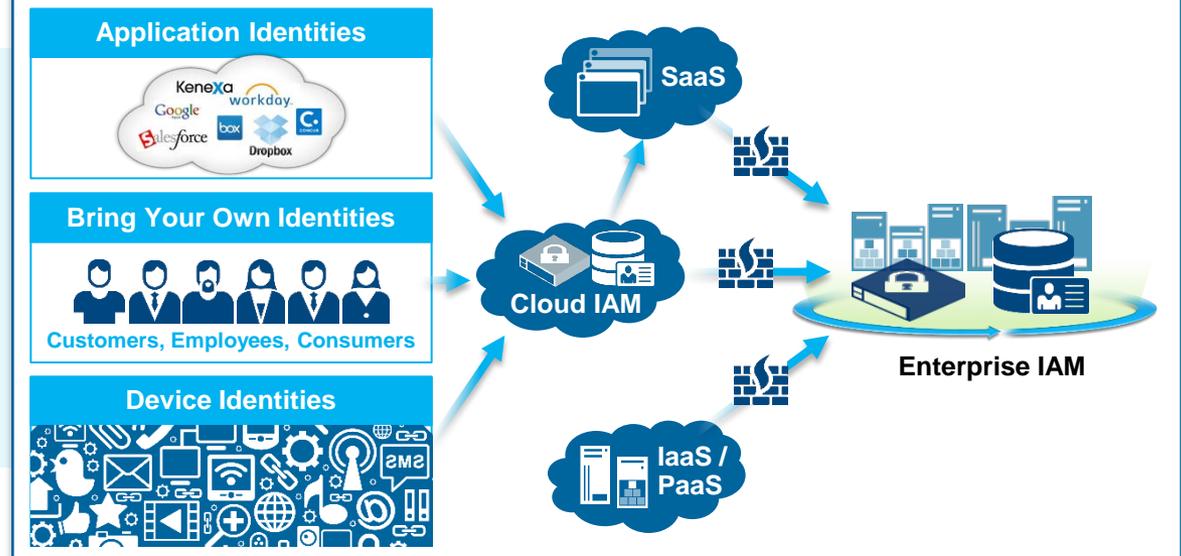
Identity and access controls are centralized and internal



Threat-aware IAM

- Security risk management
- Business driven
- Dynamic, context-based

Identity and access controls are decentralized and external



Organizations are also seeking a business-driven approach to Identity Governance and Intelligence

Identity and Governance Evolution

1 Administration

- Cost savings
- Automation
- User lifecycle
- Key on premise applications and employees

2 Governance

- Role management
- Access certification
- Extended enterprise and business partners
- On and off-premise applications

3 Analytics

- Application usage
- Privileged activity
- Risk-based control
- Baseline normal behavior
- Employees, partners, consumers – anywhere

Identity Intelligence: Collect and Analyze Identity Data



Improved visibility into how access is being utilized



Risk-based insights for prioritized compliance actions



Clear actionable dashboards for better business decision making

Threat-aware Identity and Access Management is becoming the first line of defense for securing the open enterprises



Deliver actionable identity intelligence

- **Integrated access governance & management** with identity analytics, risk-based reviews, & provisioning
- **Provide real-time user activity monitoring** with security intelligence



Safeguard mobile, cloud and social access

- **Validate “who is who”** especially when users connect from outside the enterprise
- **Proactively enforce access policies** on web, cloud, social & mobile collaboration channels



Prevent advanced insider threats

- **Manage and audit privileged access** across the enterprise and cloud-based infrastructure
- **Defend applications and data** against unauthorized access



Simplify cloud integrations and identity silos

- **Provide federated access** to cloud apps and secure online business collaborations
- **Unify “Universe of Identities”** with efficient consumer profile and directory management

Four key focus areas to address the security's weakest links

1. Deliver actionable identity intelligence

Key requirements in 2015

-  Improve visibility into access granted and utilized
-  Gain risk-based insights for prioritized compliance actions
-  Enable business managers to manage and govern their users
-  Improve security controls with business driven decisions



2. Safeguard mobile, cloud and social interactions

Key requirements in 2015

 Eliminate use of passwords to secure mobile app access

 Implement a risk-based access posture for BYOD

 Enforce identity context to access SaaS and Cloud

 Validate consumer identities for improved assurance



3. Prevent insider threat and identity fraud

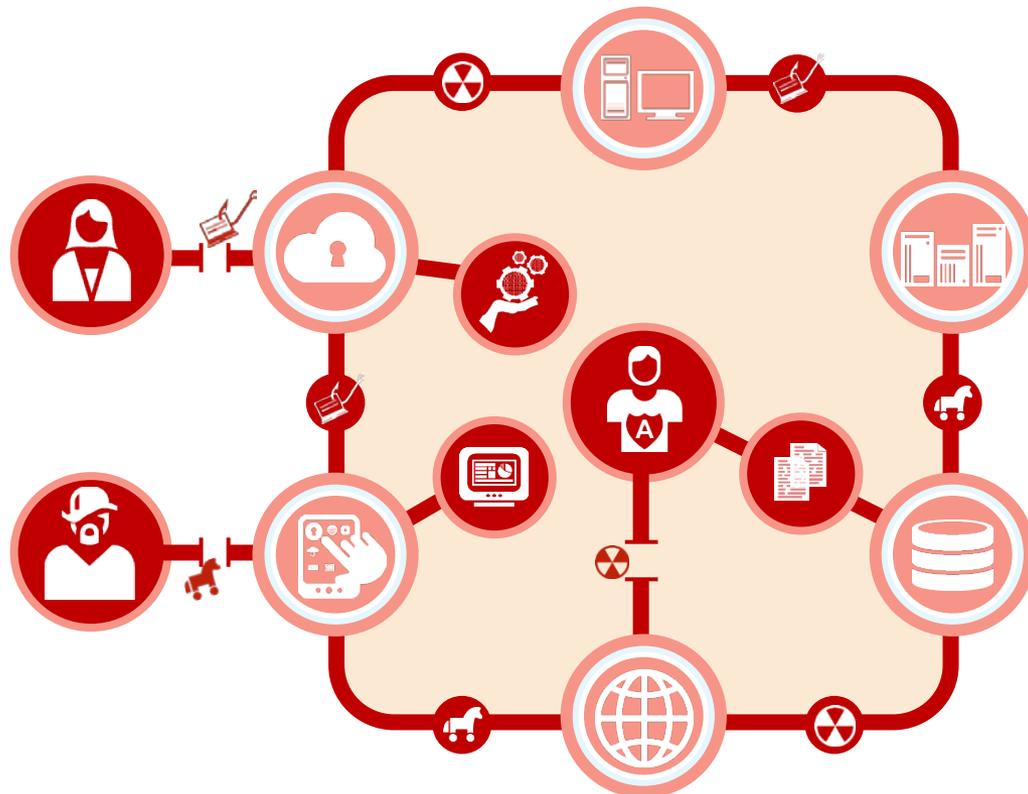
Key requirements in 2015

Control and audit shared access within enterprise & cloud

Mitigate credential theft and account takeovers with fraud & malware prevention

Secure access and protect content against targeted attacks

Correlate monitored data activity with detected anomalies



4. Simplify cloud integrations and identity silos

Key requirements in 2015

-  Enforce federated SSO to cloud and SaaS with multiple identities
-  Reduce costs of integrating and maintaining multiple identity stores
-  “Untangle” consumer identity silos to support business growth
-  Capture user insight for audit, compliance and reporting across enterprise and cloud apps



Customer successes with IBM Threat-aware IAM

Governance



Large European Insurance & financial services firm governs access to

75,000

employees, agents, privileged users

by identifying access risks, SoD & certify access for SAP, AD, Mainframe, and custom-built apps

- IBM Security Identity Governance and Administration

Mobile & Cloud



North American bank protects user access to retail and banking apps from mobile and web channels for

750K+

external users

with dynamic, risk-based access, device registration and strong authentication

- IBM Security Access Manager

Insider Threat



A Chinese manufacturer controls shared access for

600+

privileged users

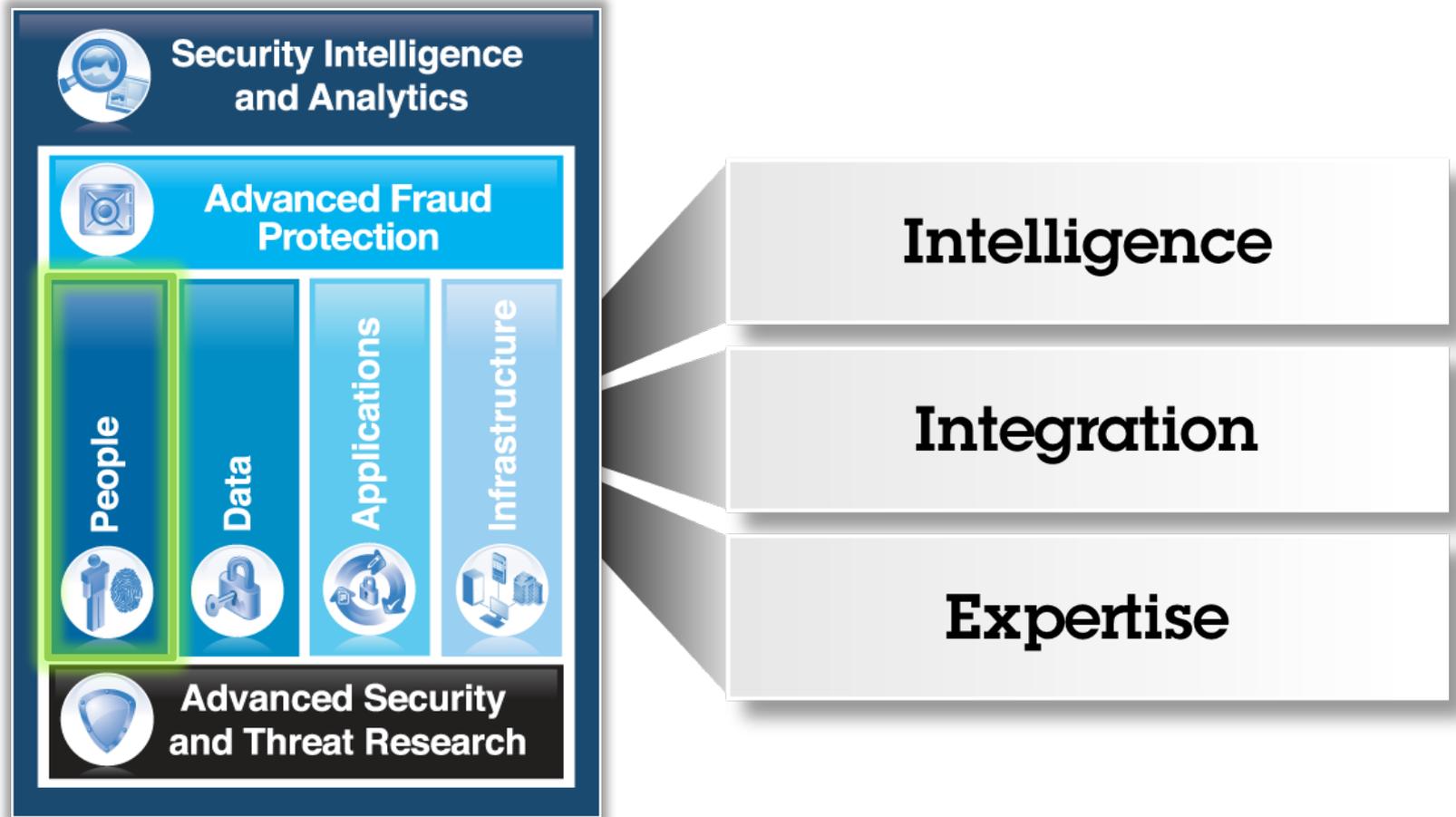
from 7 worldwide locations and controls system IDs for

2400+

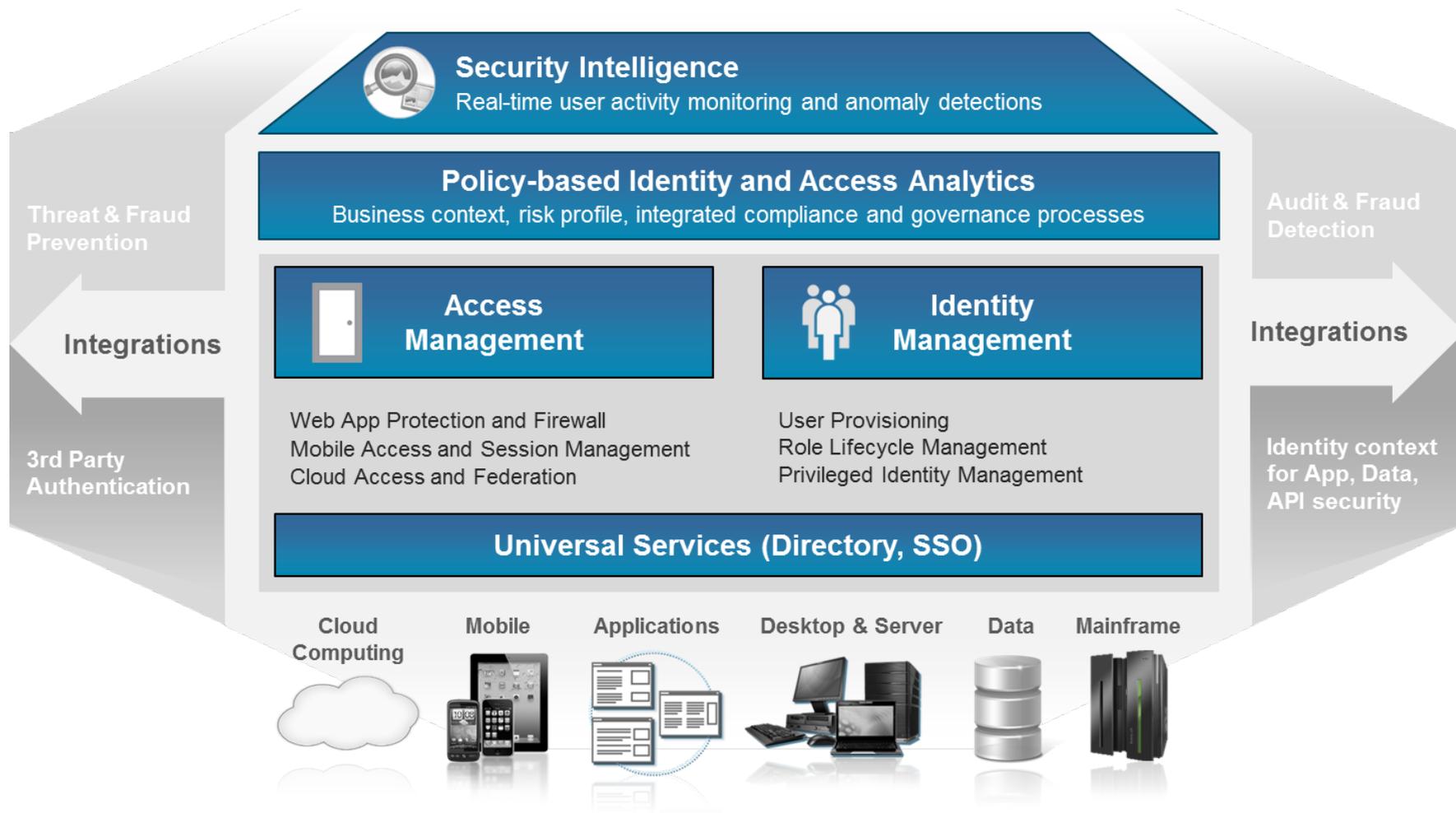
servers

- IBM Security Privileged Identity Manager

IBM Security: Delivering intelligence, integration and expertise across a comprehensive framework

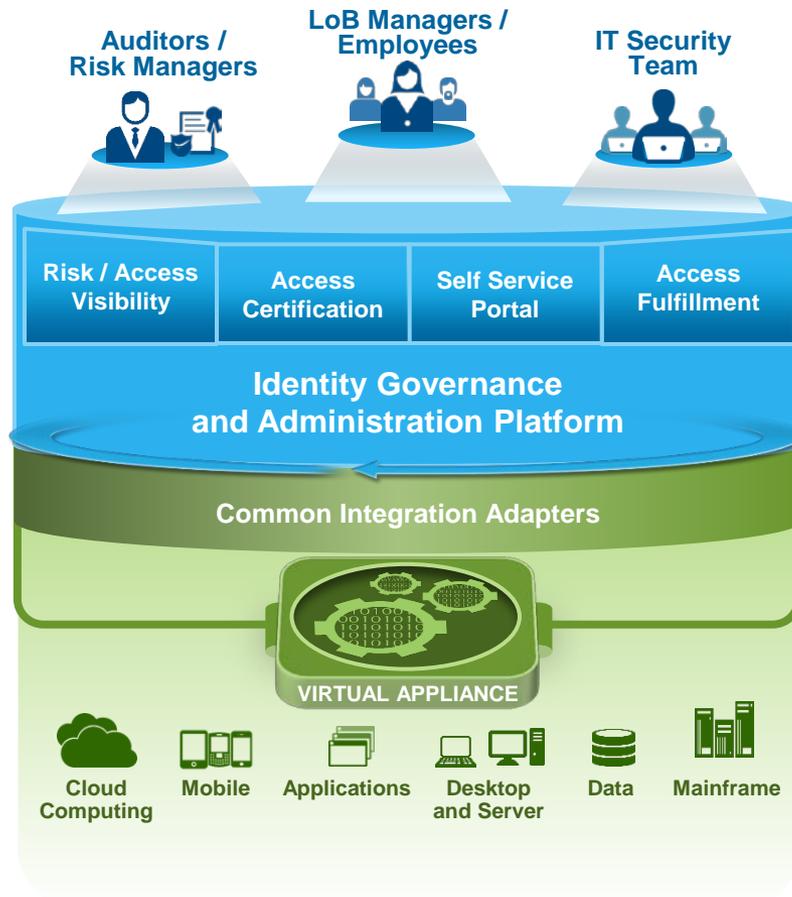


IBM Threat-aware Identity and Access Management Strategy



Manage enterprise identity context across all security domains

NEW IBM Security Identity Governance and Administration



- **Align Auditors, LoB & IT perspectives** in one consolidated identity governance & administration platform
- **Easy to launch Access Certification & Access Request** to meet compliance goals with minimal IT involvement
- **Enhanced Role Management & Separation of Duties (SoD) Reviews** using visualization dashboard and business-activity mapping
- **In-depth SAP Governance** with SoD, access risk and fine-grained entitlements reviews
- **Easy to deploy, virtual appliances for multiple customer adoptions**

NEW

IBM Security Access Management Solution

IBM Security Access Manager



The diagram illustrates the IBM Security Access Manager solution architecture. It features three stacked blue boxes representing functional layers: 'Web & Mobile Access / SSO' at the top, 'Context-based Enforcement' in the middle, and 'Web, Fraud & Malware Protection' at the bottom. A central vertical line connects these boxes. Below the bottom box is a circular icon containing a white padlock, which is positioned above a physical server rack. A large green arrow curves around the server rack, pointing from right to left, indicating a continuous or cyclical process.

Web & Mobile Access / SSO

Context-based Enforcement

Web, Fraud & Malware Protection

- **Deliver a multi-channel access gateway** to help secure employee and consumer access to mobile, web, APIs, and SaaS applications
- **Enforce identity- and context-aware application access** for web and mobile devices
- **Secure identity assurance** with built-in mobile authentication service, one-time-password use
- **Centrally manage policies** to protect enterprise from fraud and malware without modifying apps and risks associated with OWASP top 10 vulnerabilities
- **Reduce TCO and time to value** with an “all-in-one” access appliance in virtual and hardware form factors
- **Deliver built-in integrations** with Trusteer, WorkLight, Microsoft Office 365, SAP, and more



IBM Security Privileged Identity Management Solution

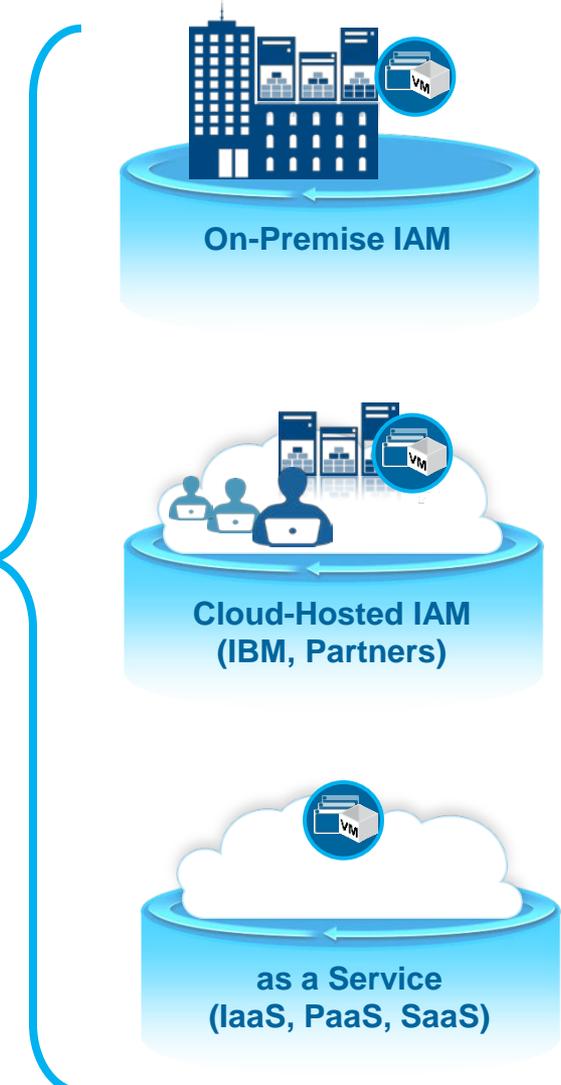
IBM Security Privileged Identity Manager



- **Privileged Identity Management for Applications** enables governance of applications/scripts credentials by replacing hard-coded passwords with automatic password check-out/check-in.
- **PIM SoftLayer cloud support** improve cloud and sensitive data security with managed administrative accounts for cloud services.
- **Virtual appliance delivery model** simplifies deployment and maintenance of privileged identity management
- **Streamlined user provisioning** and optimize maintenance of separate environments for identity & privileged identity management.
- **Simplified user experience** with administrative functions built into Identity Service Center.

Customers seeking flexible delivery models to deploy & manage IAM

IBM Security Identity and Access Management





IBM Security Cloud Authentication Solution

IBM Single Sign On for Bluemix



- **Simplified user authentication** for web applications deployed in the Cloud with a configuration-not-coding approach to security
- **Single sign-on across multiple Bluemix applications** for an improved end user experience
- **Integrate existing identity sources** by bridging security from the Cloud with on-premise enterprise directories
- **Build an authoritative identity source** with an in-cloud directory for use with Cloud applications
- **Easier security for B2C scenarios** with out-of-the-box support for popular social identity providers
- **Scalable multi-tenant platform** grows seamlessly as your business grows

NEW IBM Cloud Identity Service



Identity Management 	Access Management 	Identity Federation 
<ul style="list-style-type: none"> • User provisioning and self-service • Automated lifecycle management • Role governance and compliance 	<ul style="list-style-type: none"> • Web single-sign-on • Centralized access control policy • Strong authentication 	<ul style="list-style-type: none"> • Federated SSO • Business-to-business federation

IBM Cloud Identity Services

Solution Benefits

- Cloud-based or on premise analysis of detected security incidents
- Out-of-the-box content and automated device and network asset protection for rapid time-to-value

14M+ users

57+ countries of user origin

Millions of transactions per hour

Cloud-delivered IAM services provide a Fortune 10 client with a strategic business-to-customer (B2C) solution

Cloud-delivered Identity and Access Management (IAM)

8.5M Help secure access for internal users and external automobile customers

50K Help secure access for union workers to manage their own identities, according to union contract



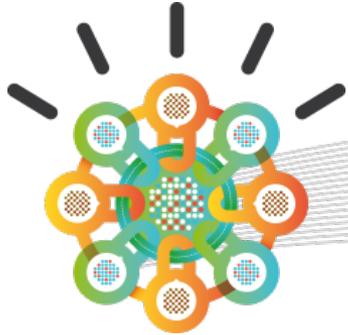
Business Challenge

- Users need multiple discrete logins / passwords to access and use different web properties
- Unable to identify and track customers to enable development of targeted offers and a more personalized web experience
- Lack of internal security skills for deploying a strategic IAM solution in house

Solution Benefits

- **Simplified web / mobile experience** via IAM integration with cloud-based social identities
- A single login providing access to a **more personalized online experience**
- **Reduced time to market** for realizing **IAM as a business enabler**
- **Agile and scalable** managed service that allows the client to “turn-on” and utilize additional services as the initiative expands globally

Learn more about IBM Security



IBM Security
Intelligence. Integration. Expertise.



Visit our website
[IBM Security Website](#)



Watch our videos
[IBM Security YouTube Channel](#)



Read new blog posts
[SecurityIntelligence.com](#)



Follow us on Twitter
[@ibmsecurity](#)

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT SYSTEMS AND PRODUCTS ARE IMMUNE FROM THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Thank You

www.ibm.com/security



© Copyright IBM Corporation 2013. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.



Ed Miller, VITA,
“Shape Up The Scene”

February 4, 2015



Virginia Information Technologies Agency

Shape Up The Scene

*Based on a security awareness
training exercise from
Northrop Grumman*

Presented by Ed Miller
ISOAG February 4, 2015



Clickers

- If you're at CESC, raise your hand if you don't have a clicker yet.
- If you're on the goto-meeting, you can still play. Instructions for that are coming up.

Clickers: SESSION ID: _ _ _ _ _

- If you are remote, you can download the clicker app to your smartphone or tablet if you haven't done so previously. Go to Google Play, Apple store, or wherever and search for "**Responseware**". It's free.
- From the Responseware APP, click the HOME button, type in the SESSION ID _ _ _ _ _ , and click JOIN.
- Alternately, you don't need an app at all. You may just use a browser and go to this URL:
- <https://www.rwpoll.com> SESSION ID is :_ _ _ _ _
- Get your Participant ID by clicking the "Information" button on the menu. In the Responseware APP the menu button looks like:





Game Rules

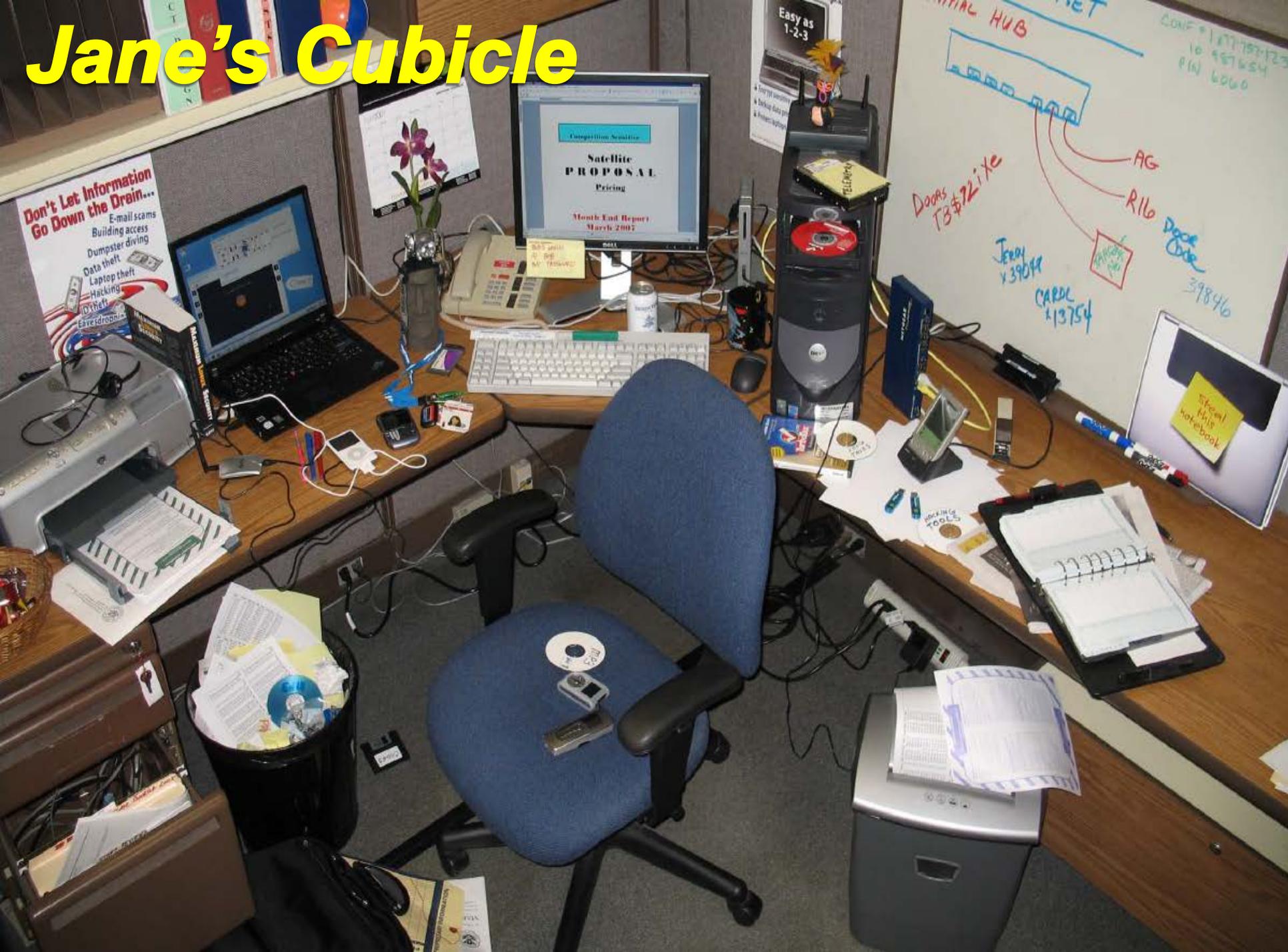
- Each question is worth 10 points, EXCEPT for the Bonus Round
- I have speed scoring turned OFF
- When a question is displayed, I will keep polling open until I think most people have answered. Just click your choice when you think you know, you can change your mind until polling is closed.
- We're playing individually. No teams this time.



The Scenario

- COV employee Jane Smith has a cubicle in a non-secure area at her agency to which many people have physical access.
- Jane had to rush off to a meeting, leaving her cubicle in disarray.
- In the process, Jane may be violating agency & COV security policies & potentially allowing for theft, loss, or compromise of COV data.

Jane's Cubicle



Don't Let Information Go Down the Drain...
E-mail scams
Building access
Dumpster diving
Data theft
Laptop theft
Hacking
ID theft
Eavesdropping

Intelligence Analysis
Satellite PROPOSAL Pricing
Month End Report
March 2007

CENTRAL HUB
CONF # 187787123
10 957654
PIN 6060
AG
R16
Doors TB522ixc
JERRY x39044
CARD x13754
Door Code 39846

Steal this notebook

WORKING TOOLS



Shape Up The Scene: Take-aways

SAVES TIME & MONEY

- The typical 1000 person office **loses approximately \$2.5 million dollars a year** from the inability to locate and retrieve information in a timely manner.
- Even more is lost in the cost of repairing or replacing lost or damaged equipment.



Shape Up The Scene: Take-aways

GOOD IMPRESSIONS

- You never know who and you never know when someone will visit your office.
- A clean and organized workspace makes your agency look efficient and presentable to anyone who decides to visit (i.e. auditors!)



Shape Up The Scene: Take-aways

COMPLIANCE

- A clear organized desk & a clear screen is a specific control requirement of the ISO 27001 information security standard.
- It also helps your agency comply with basic privacy & security best practices that ensure that personal & confidential information is kept secure.



Shape Up The Scene: Take-aways

DISCOURAGE PRYING EYES

- Leaving sensitive reports & documents out in the open or writing sensitive information on post-it-notes or whiteboards in plain view are bad security habits.
- Doing so can encourage dishonest employees, cleaning crews, and maintenance staff to view information they should not have access to.



Shape Up The Scene: Take-aways

INCREASES SECURITY

- Putting away nonessential items and documents whenever an extended absence is anticipated and securing documents and electronic media at the end of the work day will also help mitigate some of the risks associated with leaving information unprotected.



Shape Up The Scene: Take-aways

SECURE STORAGE

- You can't expect employees to maintain an organized workspace if they have no place to put their documents.
- Ensure that your agency provides adequate filing & cabinet space or other storage options.
- If the physical documents are confidential, ensure that they can be locked up!



Shape Up The Scene: Take-aways

DISPOSE OF DOCUMENTS SECURELY

- Employees should **never** throw any work-related documents or media into the trash can.
- Once it's in the trash & leaves your agency, it's out of your control. Nothing can put an agency on the front page faster than exposing sensitive information through improper disposal.
- Use a secure shredding service for disposing of documents & follow SEC514 for all media disposal.



Shape Up The Scene: Take-aways

CONTROL THE USE OF PERSONAL DEVICES

- Unknown & unauthorized devices or software may contain malware.
- Personal devices may be used to store or transfer COV data improperly, resulting in exposure of sensitive information. Be clear to employees as to what is allowed or not.
- Unauthorized devices can cause confusion, waste time, and create clutter.



Shape Up The Scene: Take-aways

RISK ASSESSMENT

- Whether or not your agency needs its own official “clean desk policy” should be based on risk.
- You should review the various business units in your agency & assess the risks associated with unattended workstations, desks & documents.
- If a policy is required, based on assessed risk, you should opt to develop one.



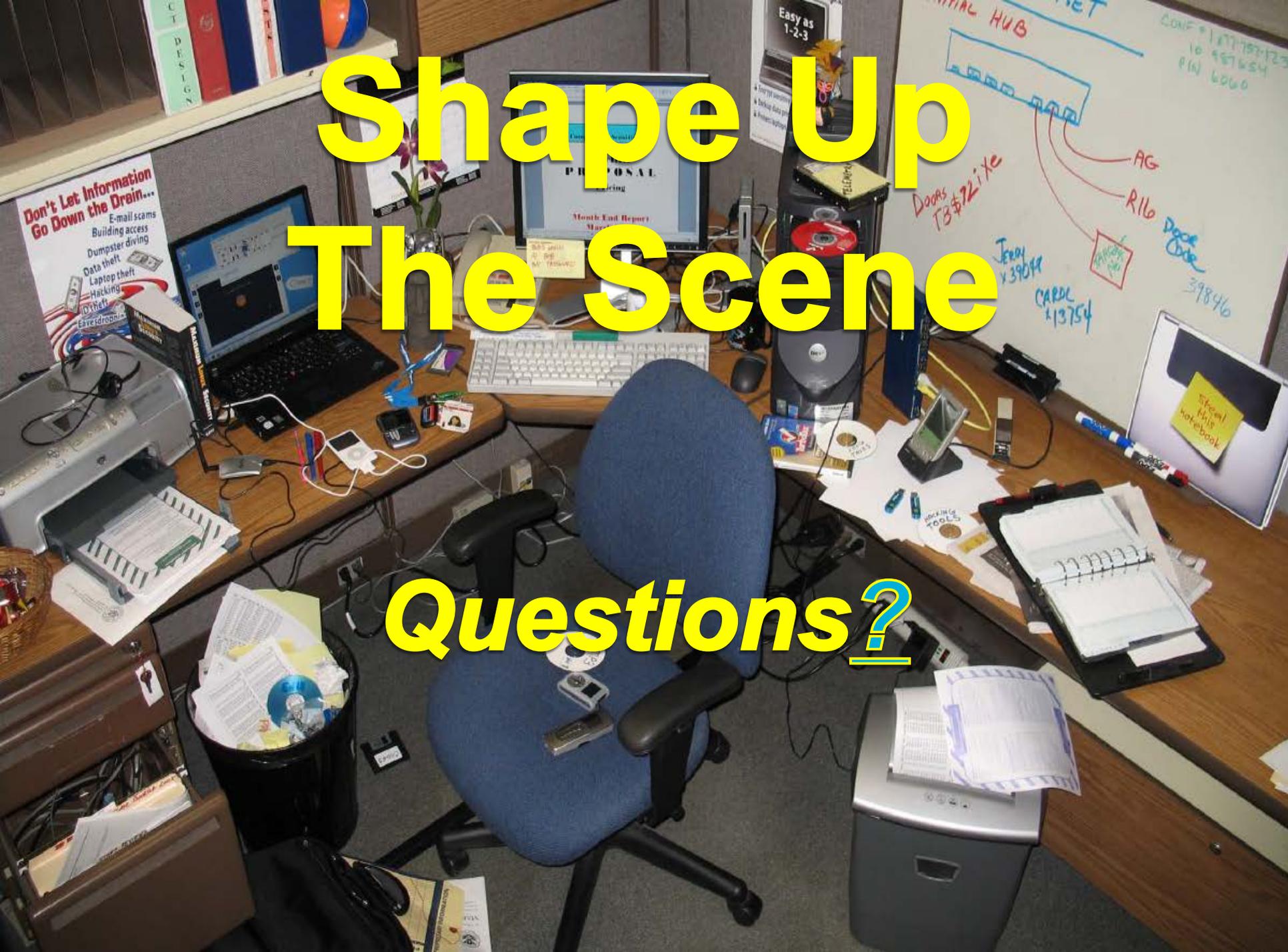
Shape Up The Scene: Take-aways

COMMUNICATE!!

- If you have identified that your agency needs this type of policy, you must communicate the policy & train your staff.
- Make staff aware about the need for the policy, the importance of adhering to the policy, & the impact of a policy breach.
- Empower employees by making them aware about the critical information that they control & their expected role in the process.

Shape Up The Scene

Questions?





Virginia Information Technologies Agency

Upcoming Events





State Governments and Cybersecurity Risks: What Are Your Next Moves?

Deloitte State Cyber Webcast

February 24, 02:00 PM ET | 1 Intermediate CPE Credit

With state governments holding increasing amounts of comprehensive citizen data, they are attractive targets for cybercrime and hacktivism. What are important implications and potential next moves for state governments to better protect against cybersecurity risks? We'll discuss:



State Governments and Cybersecurity Risks: What Are Your Next Moves?

- The complexity of cybersecurity with cyber threats and breaches crossing all levels of state government, including governors, state officials, CIOs, and CISOs.
- Key state government trends in cybersecurity budgets, strategy, and talent.
- Ideas for moving forward to keep pace with the evolving cyber threat landscape, including increased communication and collaboration with business leaders.



State Governments and Cybersecurity Risks: What Are Your Next Moves?

Learn about findings from the 2014 Deloitte-NASCIO Cybersecurity Study and innovative ways states can address cybersecurity risks going forward.

[Register](#)

To join the Dbriefs Webcasts for Industries series: [Sign up here](#) or register to attend an [upcoming webcast](#).



VT Hosting SANS class in March

- SANS SEC 511 "Continuous Monitoring & Security Operation", general course description is at <http://www.sans.org/course/continuous-monitoring-security-operations>. Chris Crowley will be the instructor.
- \$1800/person for EDU (Higher Ed, Community College, K-12, any .EDU) or state/local govt employees. \$5140 - full price for commercial or federal govt employees.

www.cpe.vt.edu/isect. This site contains the class info and registration information.



VT Hosting SANS class in March

March 9-14, 2015, 0900-1730

2150 Torgersen Hall, VA Tech, Blacksburg, VA 24060

REGISTRATION OPTIONS:

ONLINE (vLive) OPTION: If you plan on taking the class remotely, register at

<http://www.sans.org/onsite/details/38407>. Use the

DISCOUNT CODE: **PART_38407** to get the **\$1800/person price**.

ONSITE: www.cpe.vt.edu/isect. No discount code needed for onsite class.



IS Orientation

When: Thursday, March 19th, 2015

Time: 10:00 am to 12:00 pm

Where: CESC , Room 1211

Register here:

<http://vita2.virginia.gov/registration/Session.cfm?MeetingID=10>



2015 IS Security Conference

COV Information Security Conference

April 2-3, 2015

Richmond, VA



Conference Statement

IT Security Conference *“Unifying the Business Enterprise”*

- In addition to hearing expert presentations and sharing ideas with fellow managers, auditors and technical professionals around this theme, conference participants will have the opportunity to:
- **Expand their professional networks.**
- **Learn about security products and services.**
- **Maintain professional certifications.**



Who Should Attend

IT Security Conference

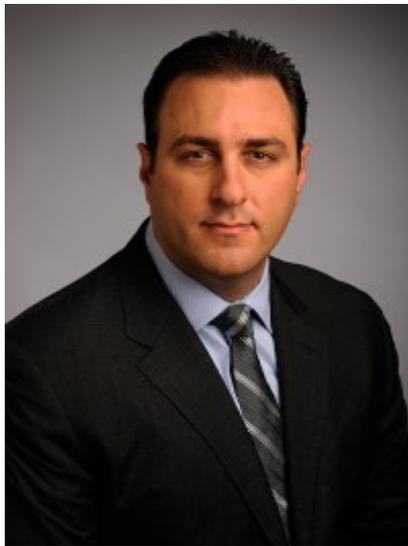
“Unifying the Business Enterprise”

- Information Security Officers
- Information Security Analysts and Engineers
- Chief Information Officers
- IT Auditors
- Privacy Officers
- Risk Officers
- Other IT officers, managers, and staff with an interest in security or privacy



Keynote Speaker – April 2, 2015

IT Security Conference *“Unifying the Business Enterprise”*



Michael Fey

**President and Chief
Operating Officer
BlueCoat**

Keynote Speaker – April 3, 2015

IT Security Conference *“Unifying the Business Enterprise”*



Karen Evans

**Director for the US Cyber Challenge
(USCC).**



Conference Topics Day One

Dan Han (VCU) - Managing regulatory compliance in a non-compliant world

Tom Bowers ((ePlus) - The Shared ISO model

Karen McDowell (UVA) - Business, Information Security, and the Internet of Things

Shana Bumpas (TAX) – PCI

Scott K. Hammer (Driving Value with Information Security Compliance

Jean Rowe (Bitreserve Inc) - ORMS Bootcamp

Andrea Di Fabio (NSU) - Sharing sensitive information in a more secure manner

Doug Streit (ODU) - IT Security Governance - One ISO's journey

Note: Topics are subject to change prior to conference



Conference Topics Day One (Con't)

Michael Light (AT&T) - BigData and (In)Security Considerations

Randy Marchany (VTECH) - Continuous Monitoring Challenges

Peter Allor (IBM) - Security Threats, Frameworks, and Mitigation Efforts How
Can You Lower Your Risk?

Eric Adkins (Verizon) - Data Breach Security

Note: Topics are subject to change prior to conference



Conference Topics Day Two

Peter Aiken (VCU) - Data - How can you secure it if you can't manage it?

Lorne Joseph (eGRC.COM) - Bringing Governance to Government

Hemil Shah (eSphere Security Solutions Pvt Ltd) - Stop throwing generic security requirement - Who has time!!!

Chandos Carrow (VCCS)- Vulnerability Scanning

Eric Bowlin (Deloitte) - Into the Cyber Security Breach

Karen L. Cole (Assura, Inc.) - Enterprise Risk Management (ERM): Unifying the Organization and Improving Performance Through Shared Management of Risks

Michael Bruemmer (Experian) - Data Breach Resolution Lessons Learned from Mega Breaches

Katie Hutchison (Box) - Cloud as a Security Solution

Jake Kouns - Risk Based Security Vulnerability Stupidity: How Do We Move Towards Intelligence?

Note: Topics are subject to change prior to conference



Conference Statement

IT Security Conference

“Unifying the Business Enterprise”

- In addition to hearing expert presentations and sharing ideas with fellow managers, auditors and technical professionals around this theme, conference participants will have the opportunity to:
- **Expand their professional networks.**
- **Learn about security products and services.**
- **Maintain professional certifications.**



Vendor Attendees

IT Security Conference

“Information Security Enabling the Business”

Verizon
Appscour
CAS Severn
Chenega Logistics
Assura Inc.
Sun Management

ePlus Technology
Cisco
SHI
Awareity
Data Network
Solutions
FishNet Security



Registration Cost

IT Security Conference *“Unifying the Business Enterprise”*

Registration fee: \$125.00 for Attendees

Note: Space is limited. Please register early.....



How To Register

IT Security Conference *“Unifying the Business Enterprise”*

You may register for the conference at the following link:

Website Link:

<http://www.vita.virginia.gov/2015COVASECURITYCONFERENCE/>



Payment Method

IT Security Conference *“Unifying the Business Enterprise”*

You may pay for the conference by: **Credit Card**
Check

If you have questions, contact:
CommonwealthSecurity@vita.virginia.gov



Future ISOAG

March 4th, 1:00 - 4:00 pm @ CESC

Speaker: Steve Werby with Altria

ISOAG meets the 1st Wednesday of each month in 2015



Submit Events

- If your group or organization is promoting a security related event and would like to have it communicated to the Information Security Officer community:

Please submit all upcoming events to:

CommonwealthSecurity@VITA.Virginia.Gov



ISOAG-Partnership Update

*IT Infrastructure Partnership Team
Bob Baskette*

4 February, 2015



NORTHROP GRUMMAN



Partnership Q & A

Bob Baskette

4 February, 2015



NORTHROP GRUMMAN



ADJOURN

THANK YOU FOR ATTENDING

