



# Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

---

June 3, 2015



# ISOAG June 3, 2015 Agenda

- |   |  |
|---|--|
| <b>I. Welcome &amp; Opening Remarks</b>   | <b>Michael Watson, VITA</b>                  |
| <b>II. Secure, Protect, and Enable;<br/>Security 101, Proactive Measures<br/>for VITA to increase IT Security</b> | <b>William Harrod, CA Technologies</b>       |
| <b>III. Archer Update</b>   | <b>Ed Miller/Mark Martens, VITA</b>          |
| <b>IV. Upcoming Events</b>  | <b>Bob Baskette/Michael Watson, VITA</b>     |
| <b>V. Partner/Operation Update</b>  | <b>Bob Baskette, VITA, Michael Clark, NG</b> |



# Welcome and Opening Remarks

**Michael Watson**

**June 3, 2015**



# Secure, Protect, and Enable; Security 101, Proactive Measures for VITA to increase IT Security

William Harrod, CA Technologies



# Secure, Protect and Enable The Virginia Information Technologies Agency



June 2015

© 2015 CA. All rights reserved.

# Welcome! What's in this for you?

- Opening remarks
- Learning Opportunity
- Security Trends today
- Security 101 – Blocking and Tackling
- Security “Stuff”
- Privileged Identity Management
- Open Discussion - Anytime





# Today, Every Organization is a Software Company.

Today, VITA must start thinking like a “tech” company, because within a few years, if not already, digital requirements will dominate. Urgent action is needed to keep up with the requirements, and to safe guard the digital records and transactions of the state.

Gartner; “CEO Resolutions for 2014—Time to Act on Digital Business”; Mark Raskino; March 5, 2014



VITA can be a leader  
in providing secure,  
seamless, access to  
support Citizens,  
Business, and  
employees



**2015 SESSION [Senate Bill 1121] VIRGINIA ACTS OF ASSEMBLY — CHAPTER**  
***An Act to amend and reenact § 2.2-603 of the Code of Virginia, relating to IT responsibility of agency directors*** The director of every department in the executive branch of state government shall be responsible for securing the electronic data held by his department and shall comply with the requirements of the Commonwealth's information technology security and risk-management program as set forth in § 2.2-2009.

New York Times – December 11, 2014

“Hacked vs. Hackers: Game on

**SONY**

Hacking attacks increased 62% in 2013

552 million people had their identities stolen

Layered security is key

There are two types of companies left in the United States:

Those that have been breached

Those that have been breached but don't know it yet



Source: <http://nyti.ms/12pWnJB>

# Technology Trends

**OVER 1.7 BILLION CONSUMERS WITH SMART PHONES BY 2018<sup>1</sup>**

**USER LOCATION AVAILABLE FOR AUTHENTICATION**

**MOBILE AUTHENTICATION AND SECURITY WILL BECOME HUMAN-FACTOR FRIENDLY<sup>2</sup>**



1) Statista "The Statistics Portal" [www.statista.com](http://www.statista.com), 2) Forrester Top 15 Trends S&R Pros Should Watch: 2014, Trend No. 14

# The Mobile Landscape is changing quickly too



# What I “hear”

- ✓ Multiple, disparate authoritative sources related to identity and attributes
- ✓ Inconsistent and manual processes for
  - ✓ provisioning/ de-provisioning
  - ✓ certification of user accounts and entitlements
  - ✓ auditing and reporting on controls
- ✓ It is difficult to determine who has access to what - when evaluating entitlements
- ✓ Multiple security silos, procedures, and controls
- ✓ Too Many Passwords, especially for Privileged Users Administering Servers
- ✓ **Lack of Automation for Single-Sign-On, Federation, RBAC, ABAC, Multi-Factor Authentication**

# STUFF

Financial /  
Payroll

Medical Records  
(HIPAA)

STUFF

PII

Tax &  
Payment  
Records

HR Info

Financial /  
Payroll

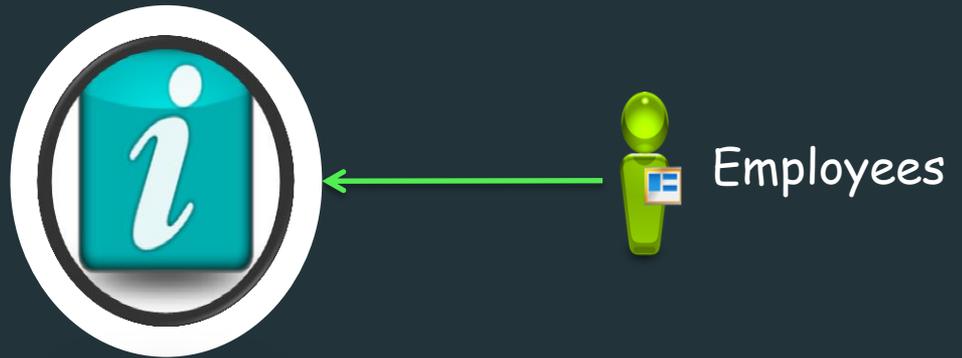
Medical  
Records  
(HIPAA)



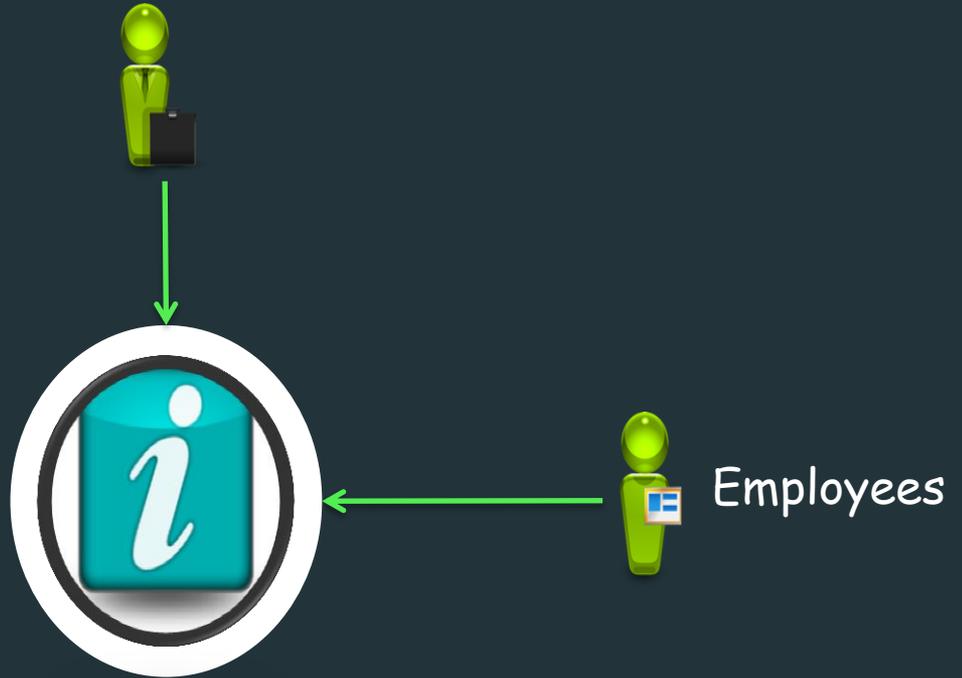
PII

Tax &  
Payment  
Records

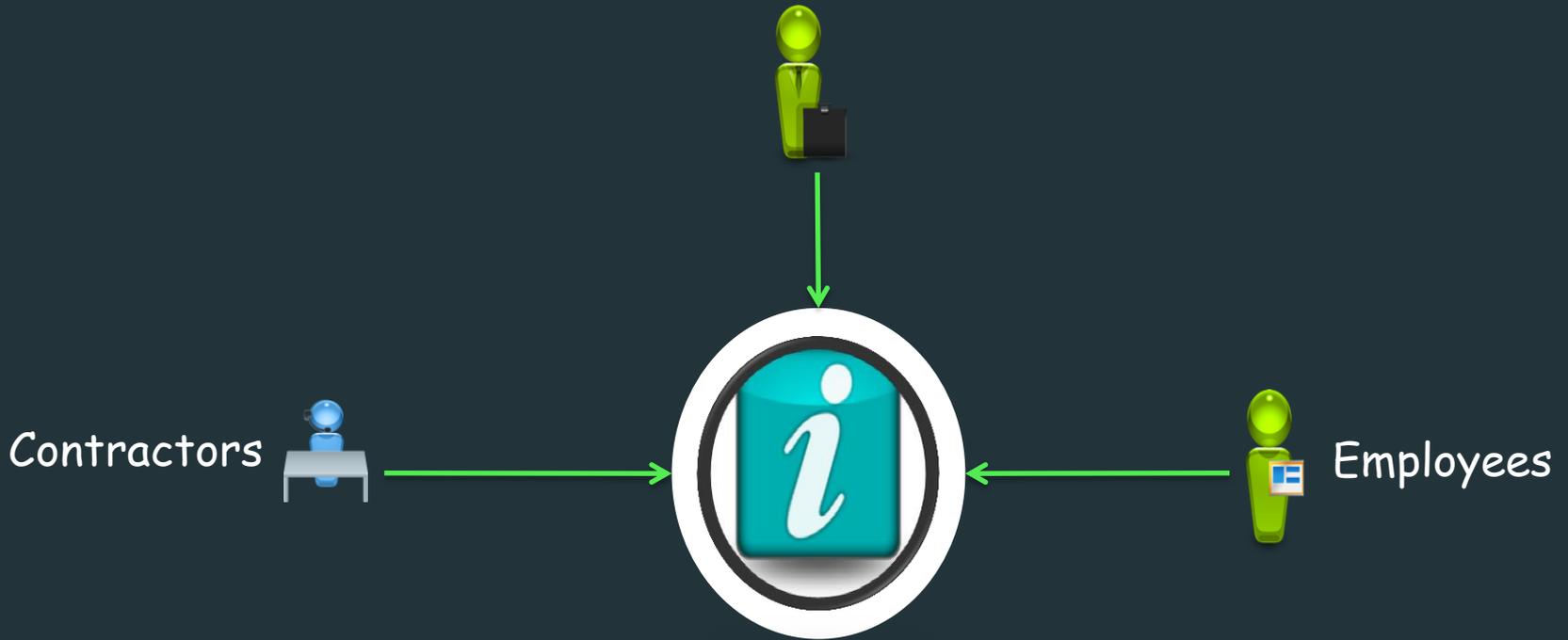
HR Info



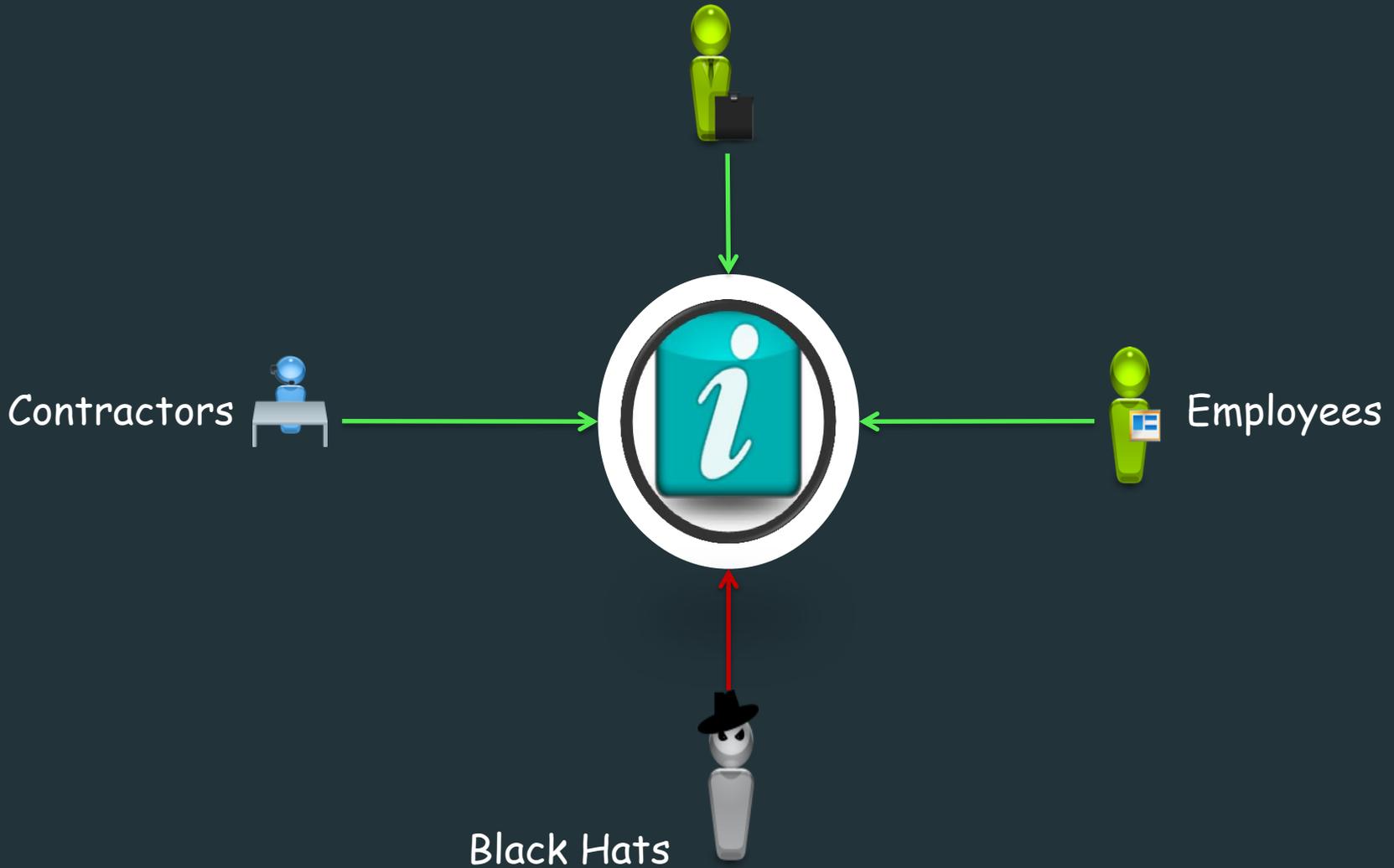
# Citizens



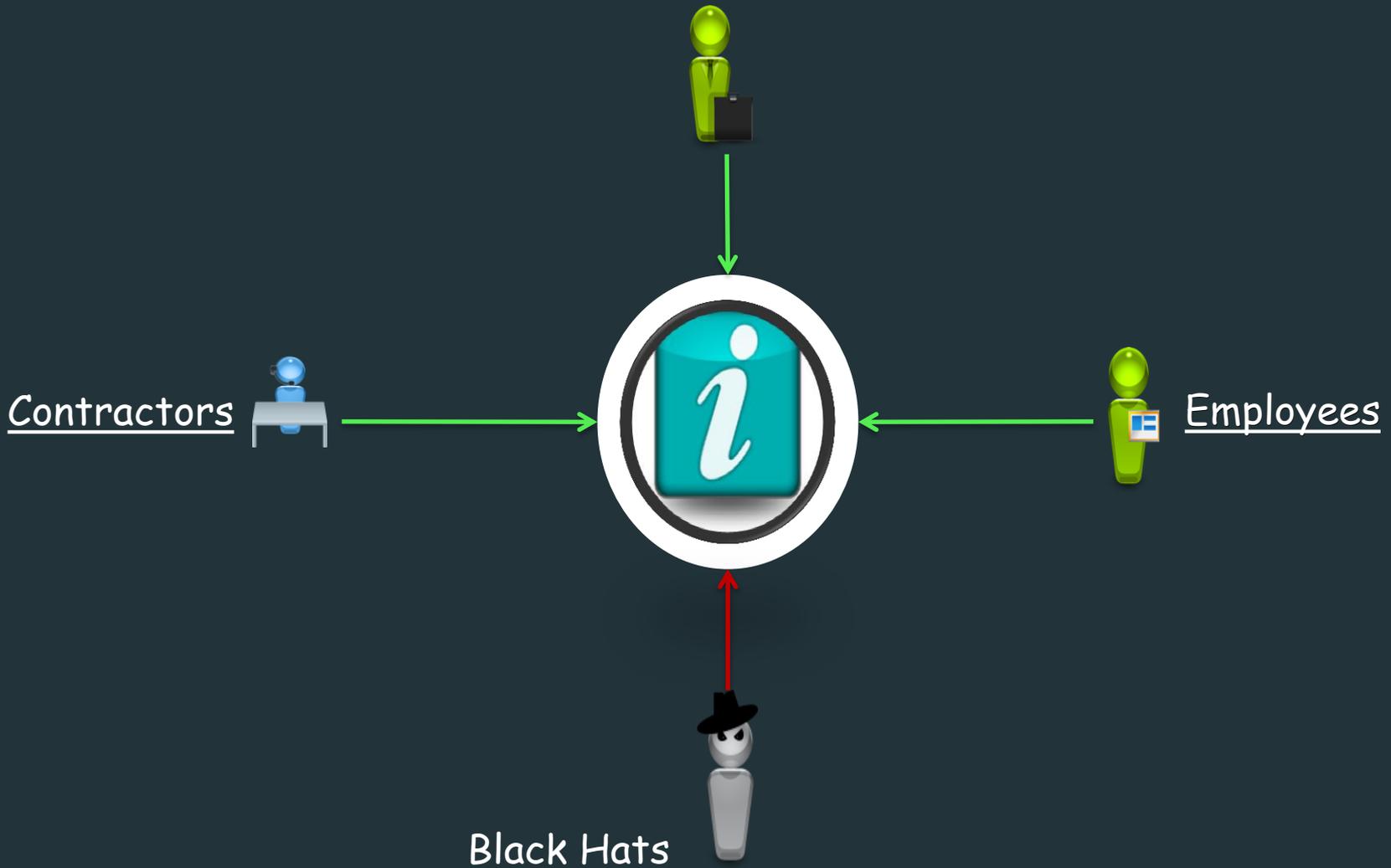
# Citizens



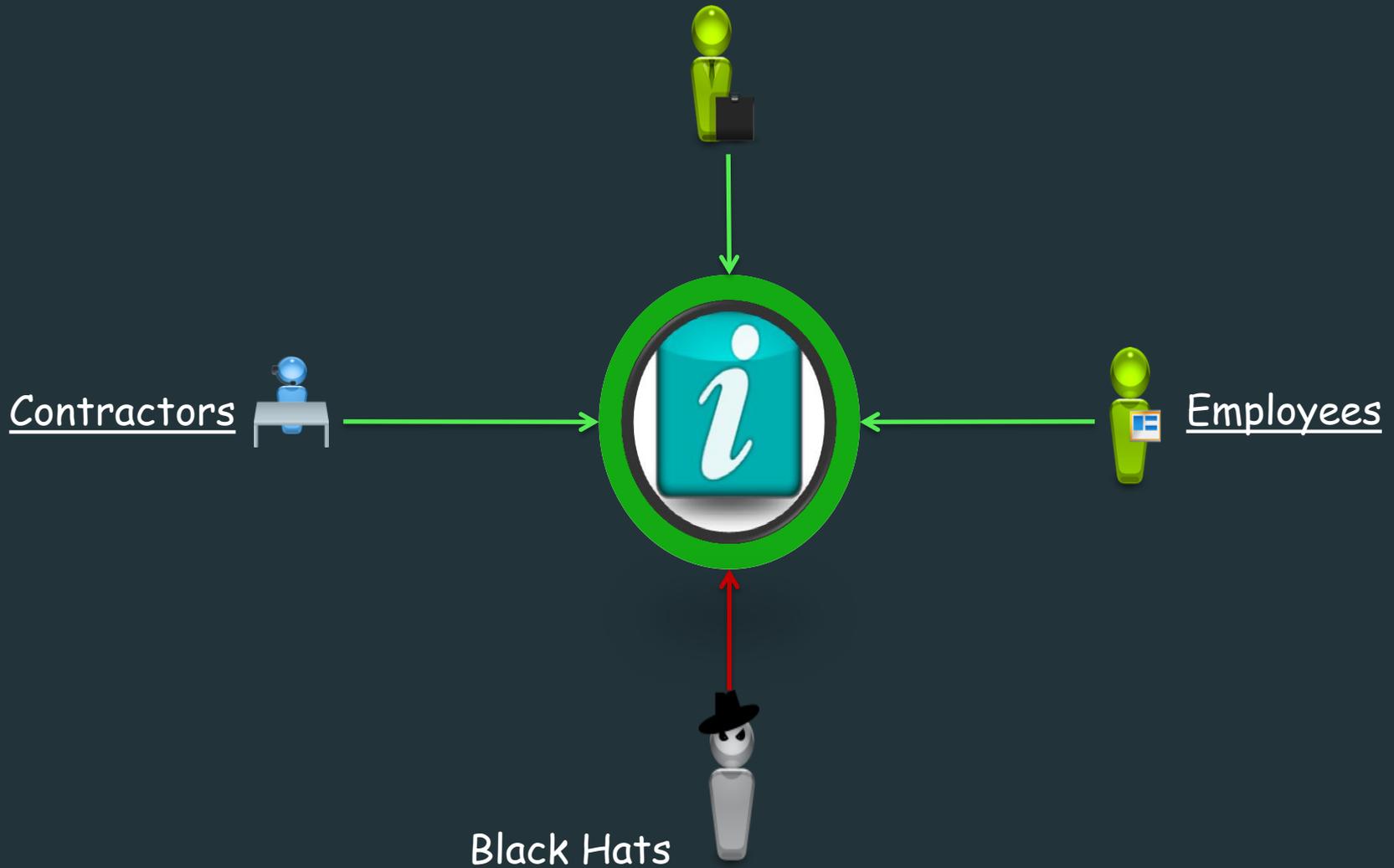
Citizens



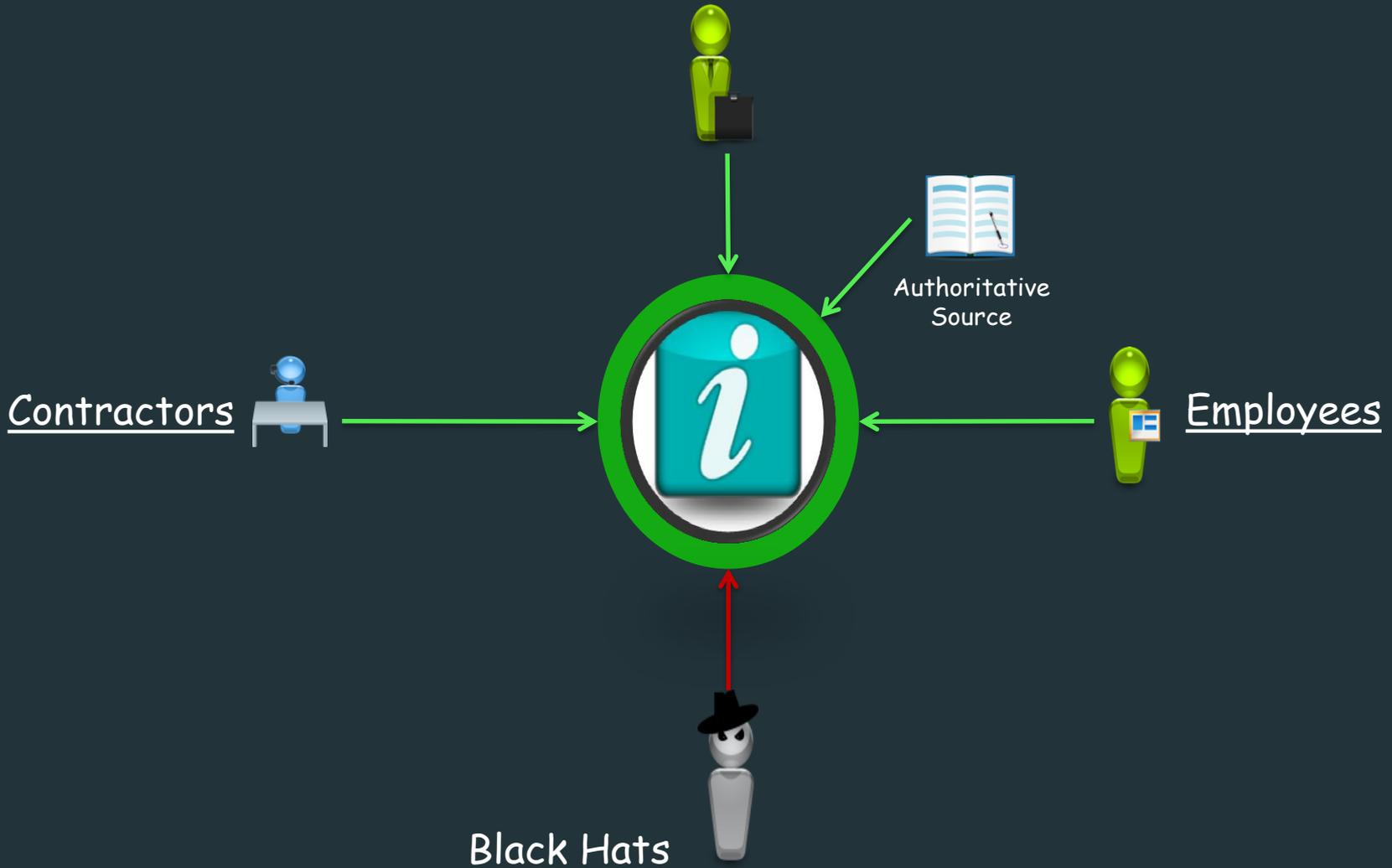
# Citizens



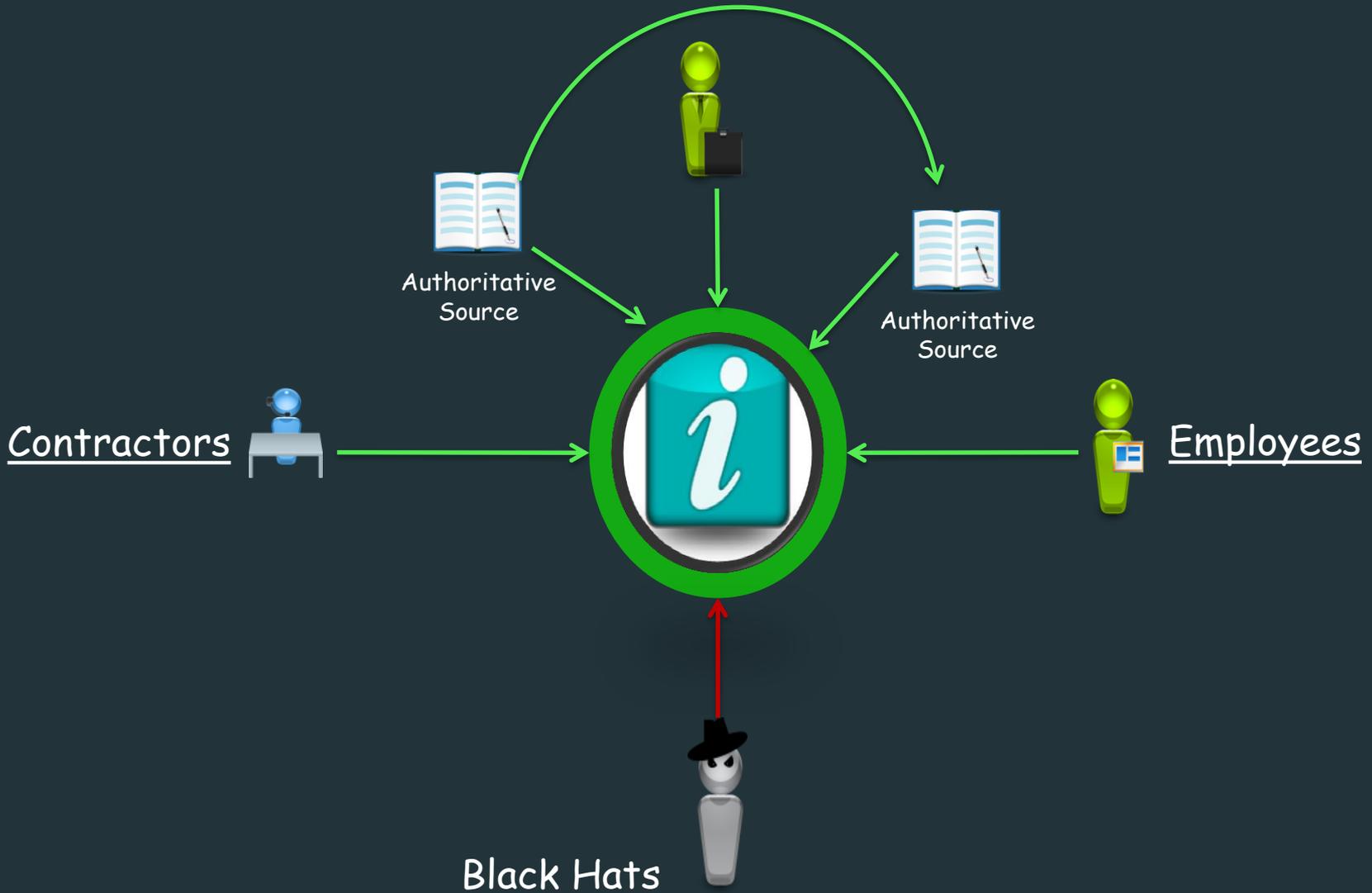
# Citizens

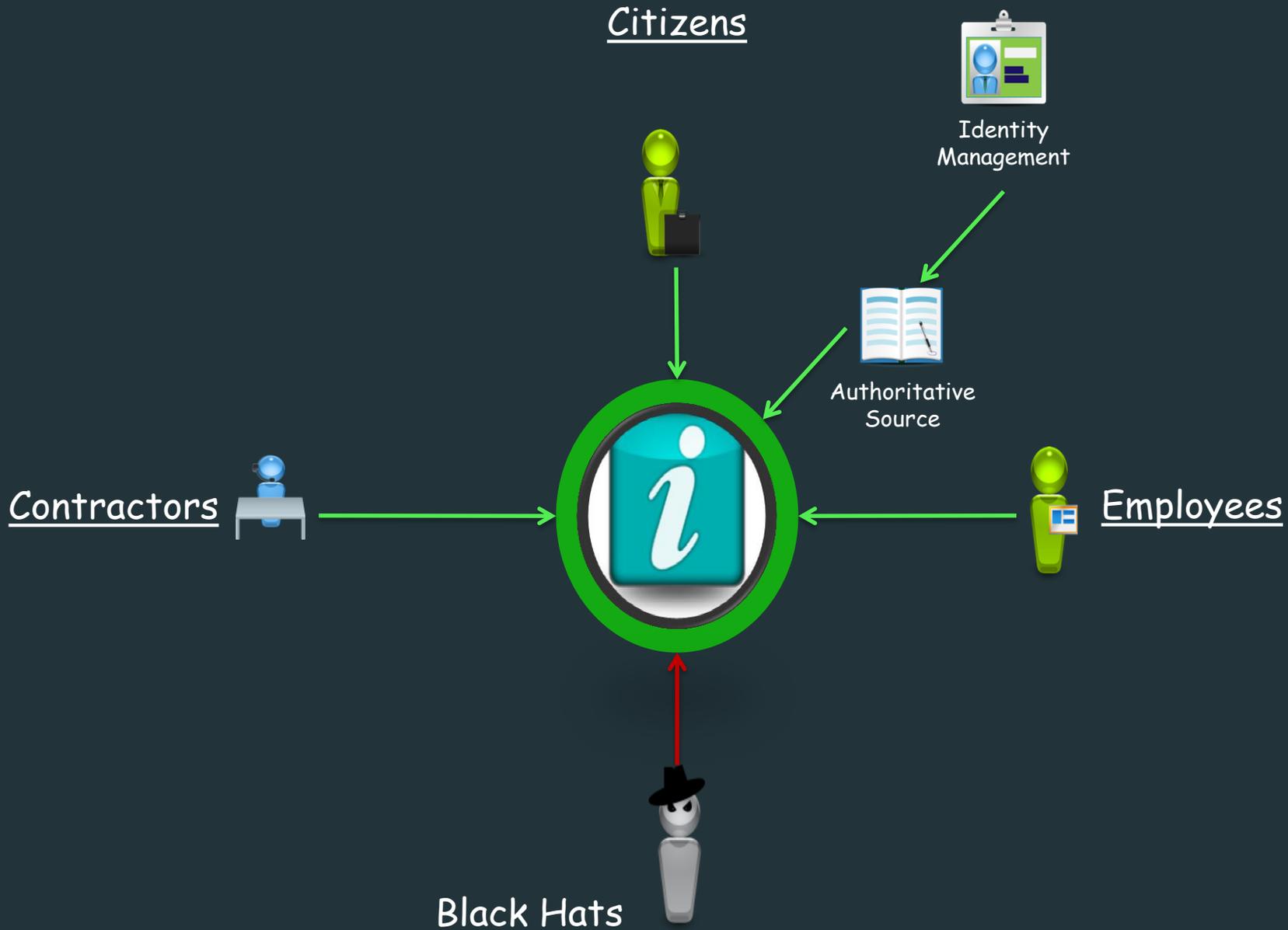


# Citizens

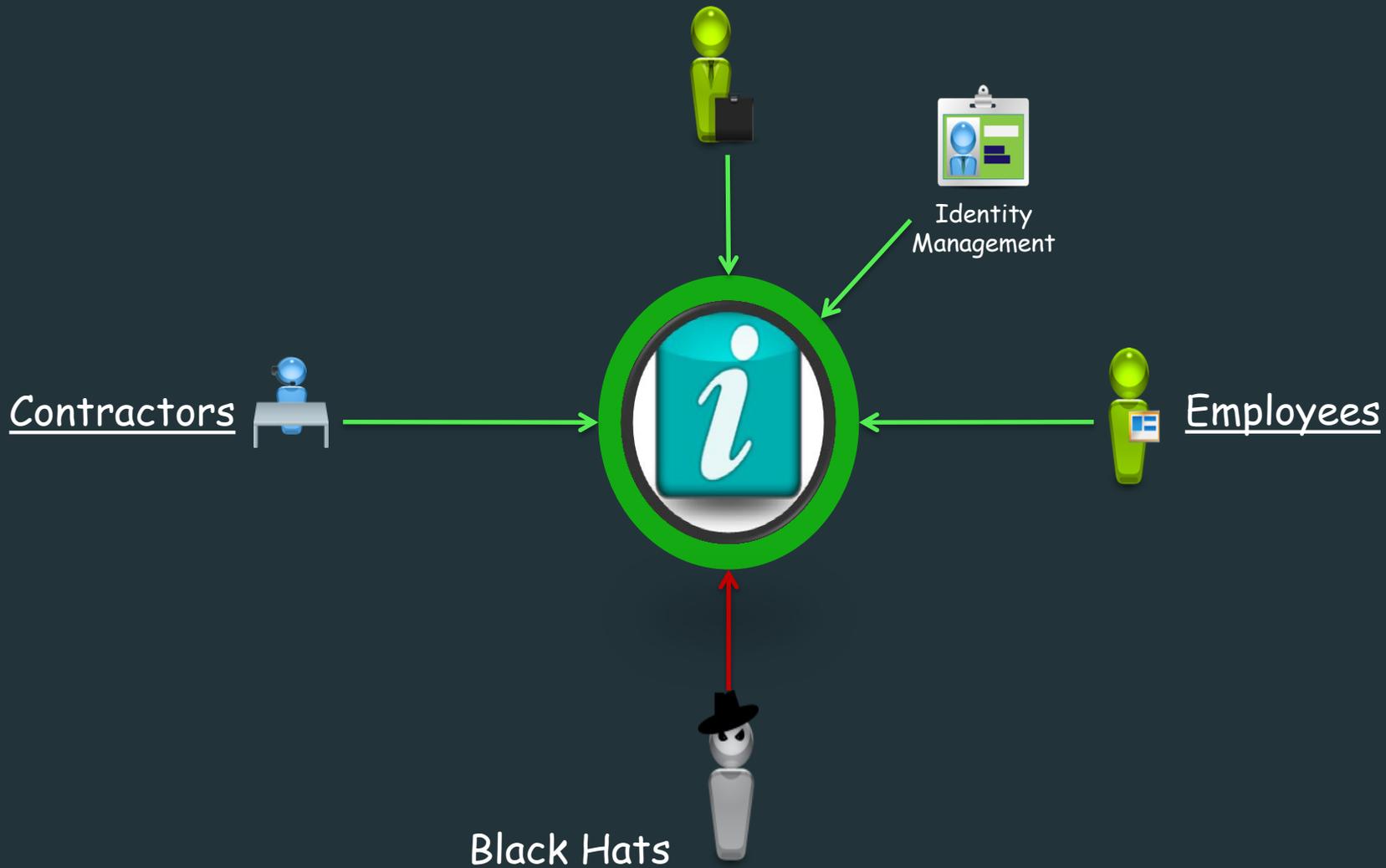


# Citizens

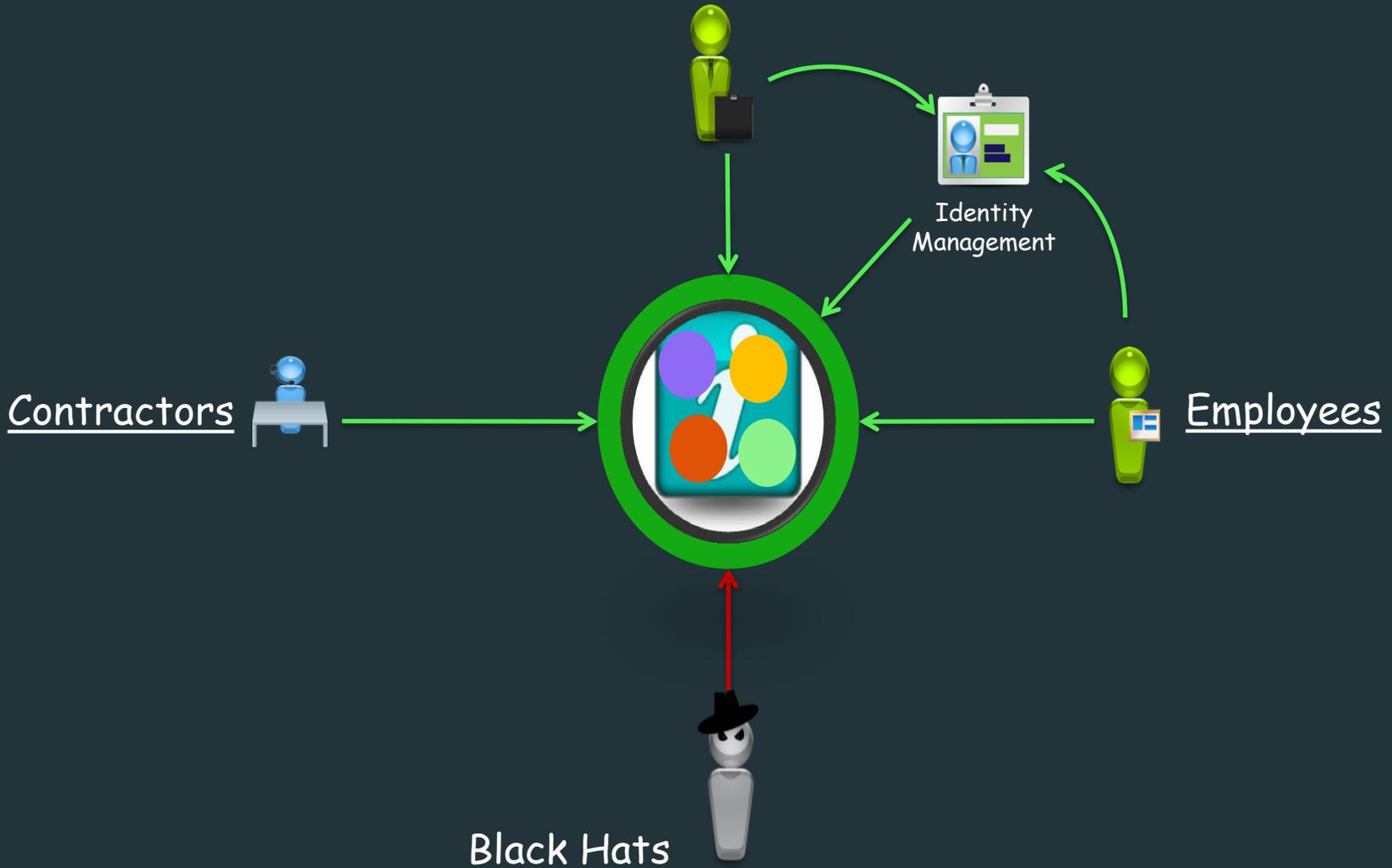




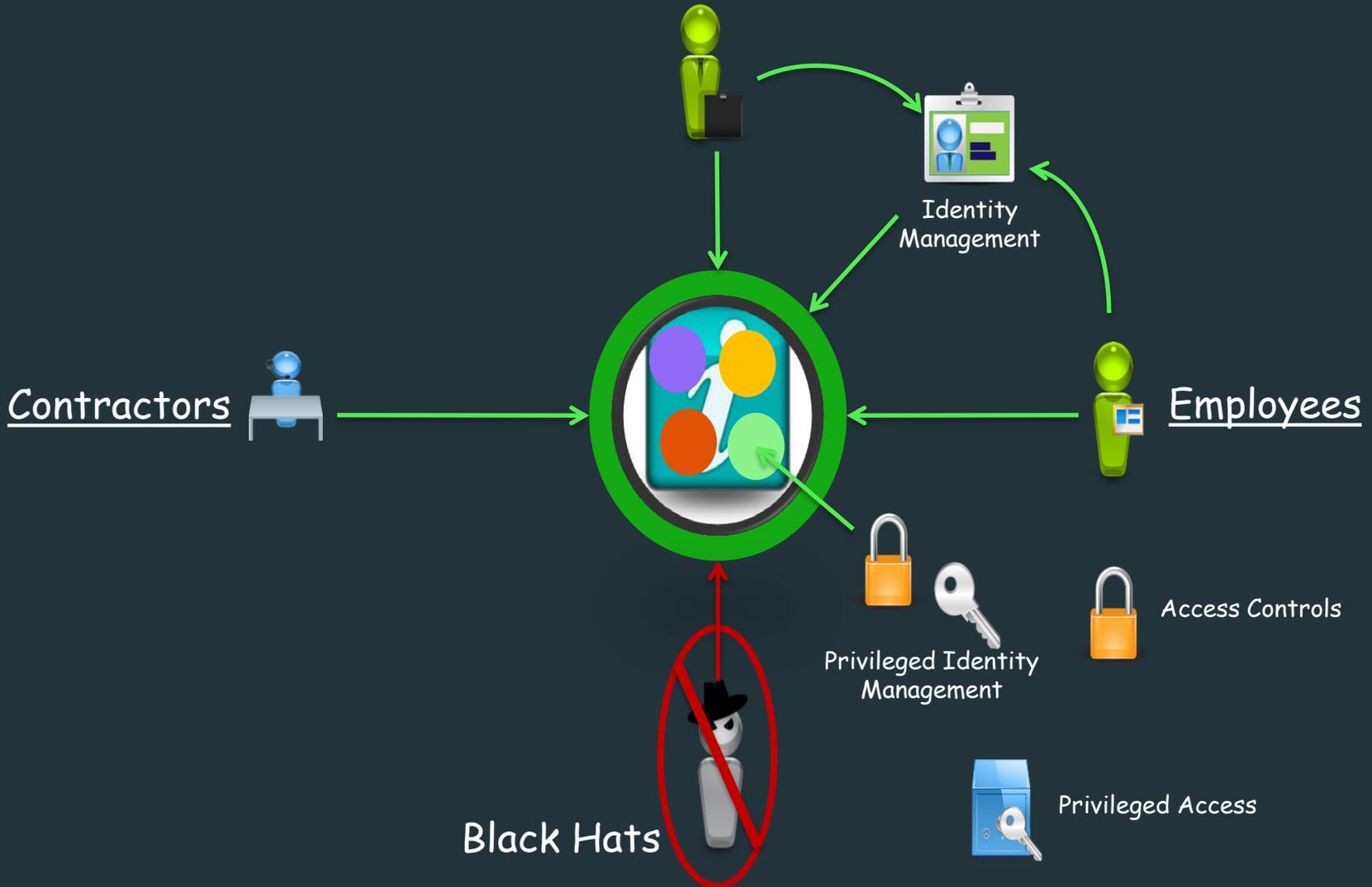
# Citizens



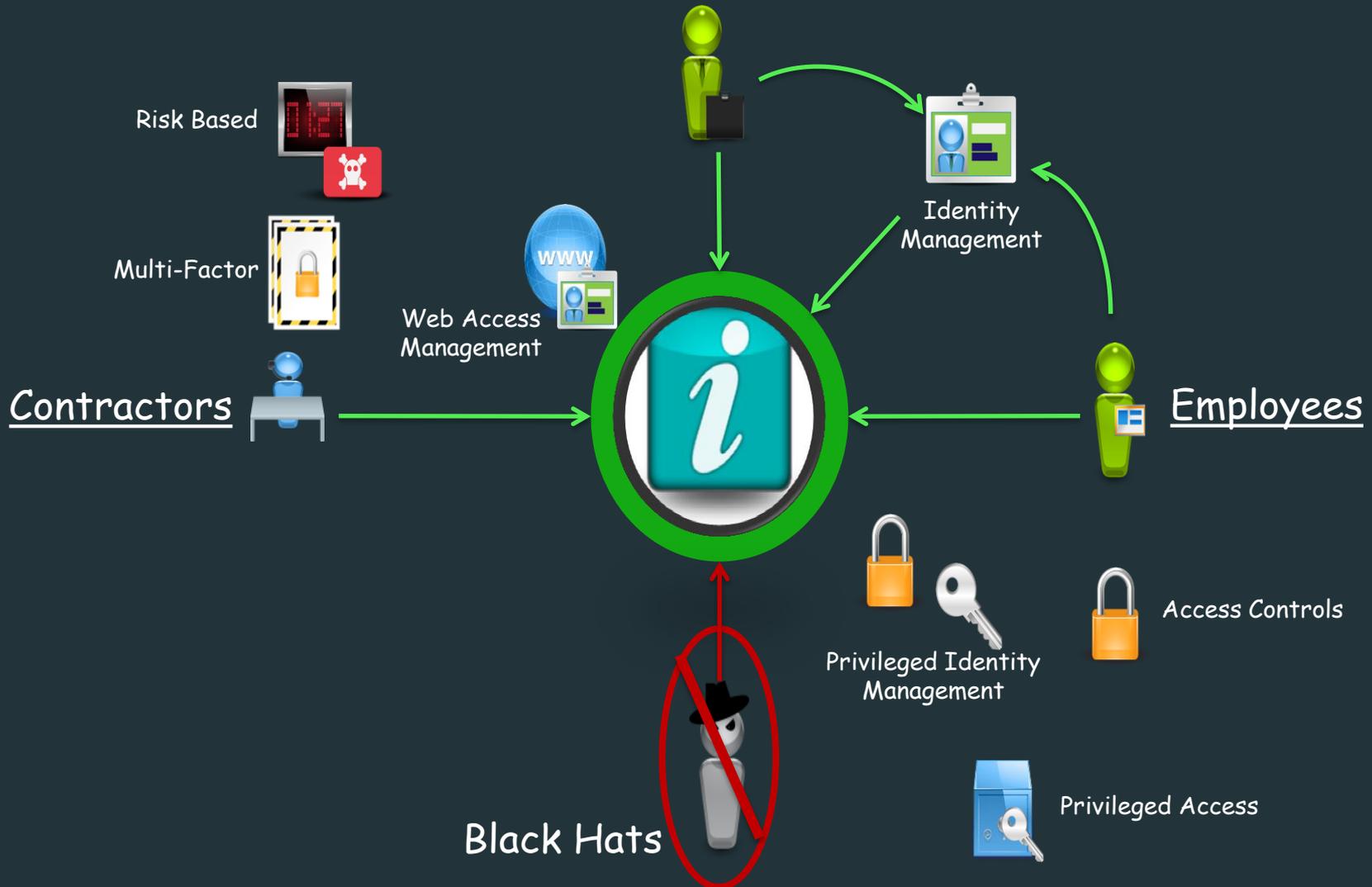
# Citizens



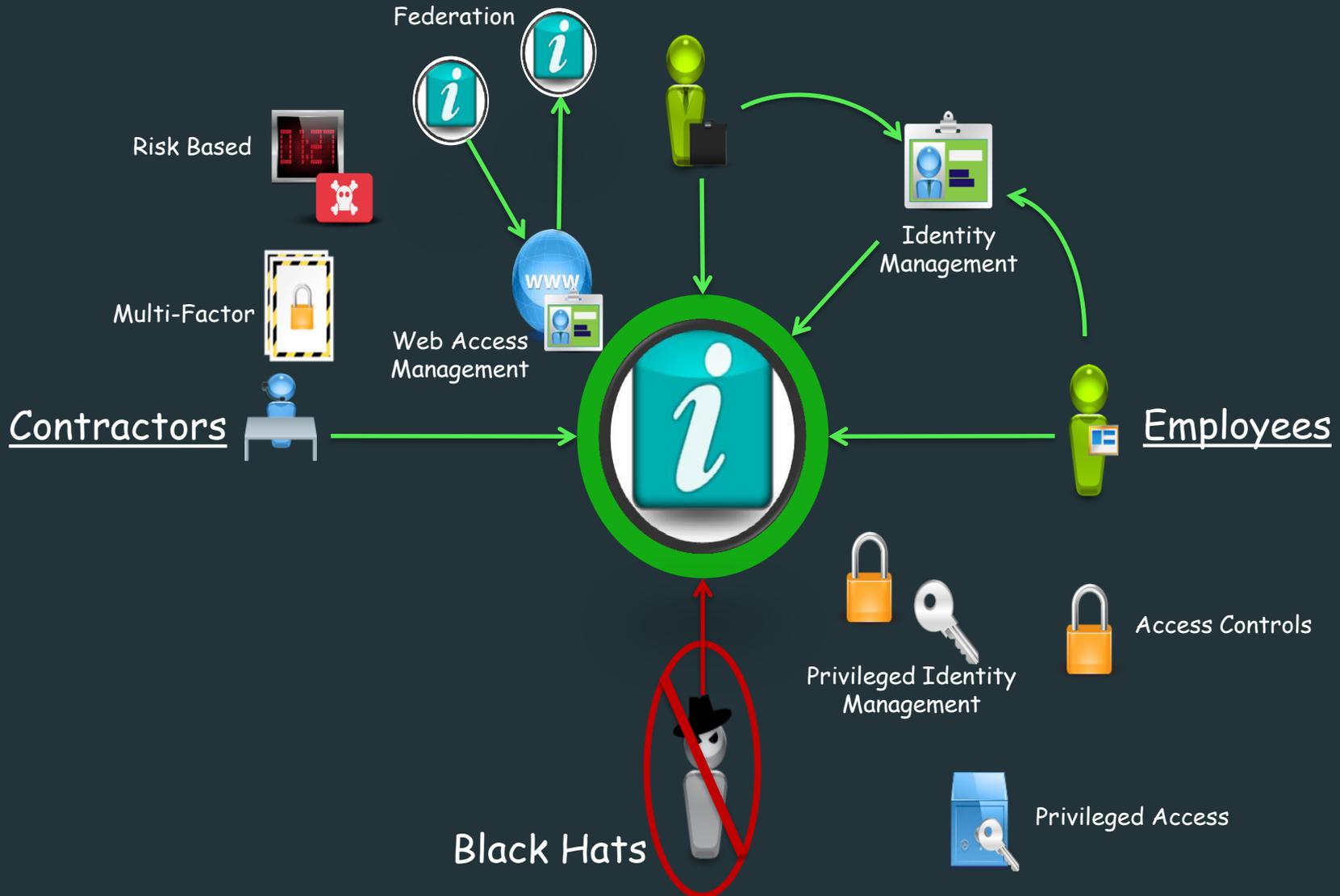
# Citizens



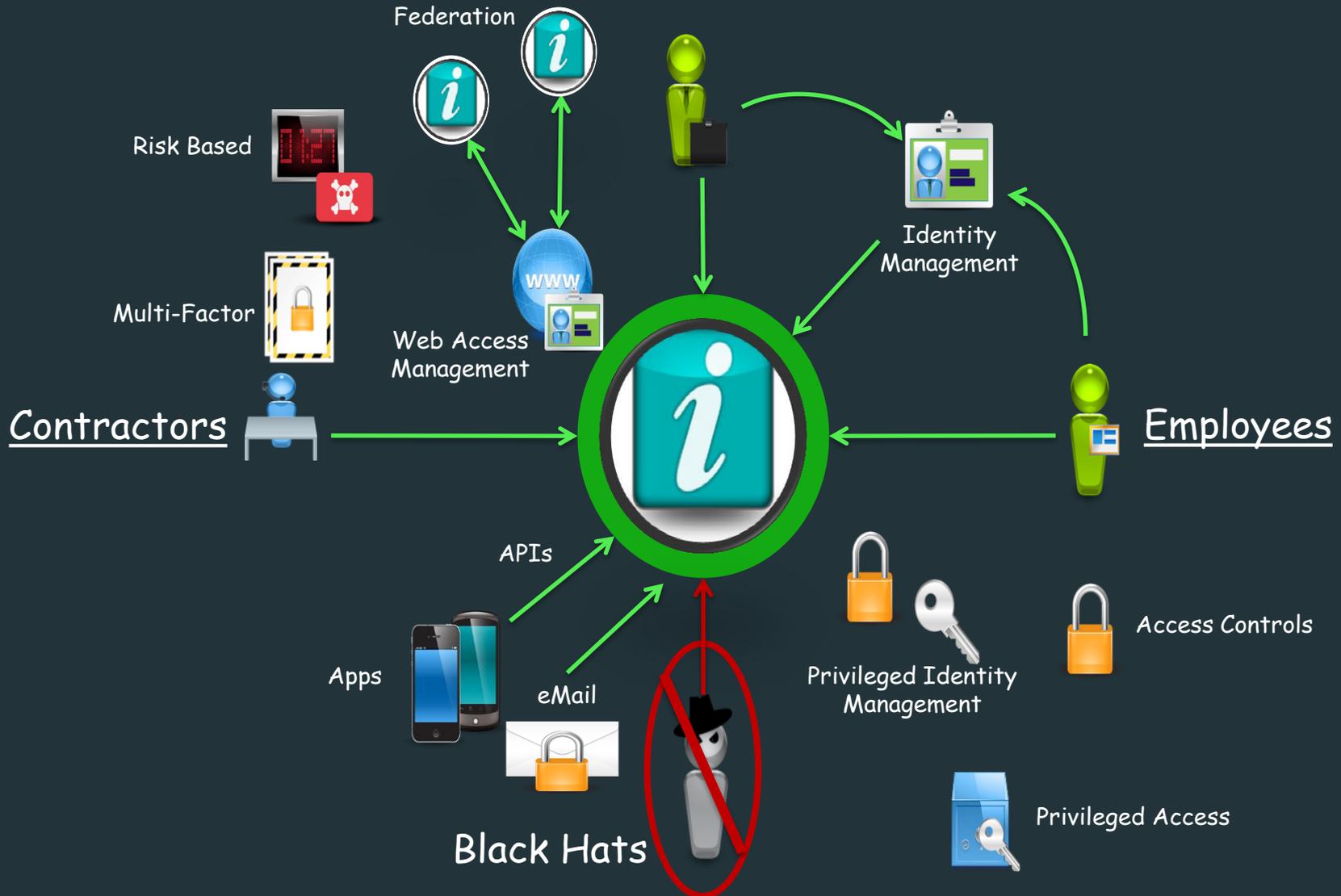
# Citizens



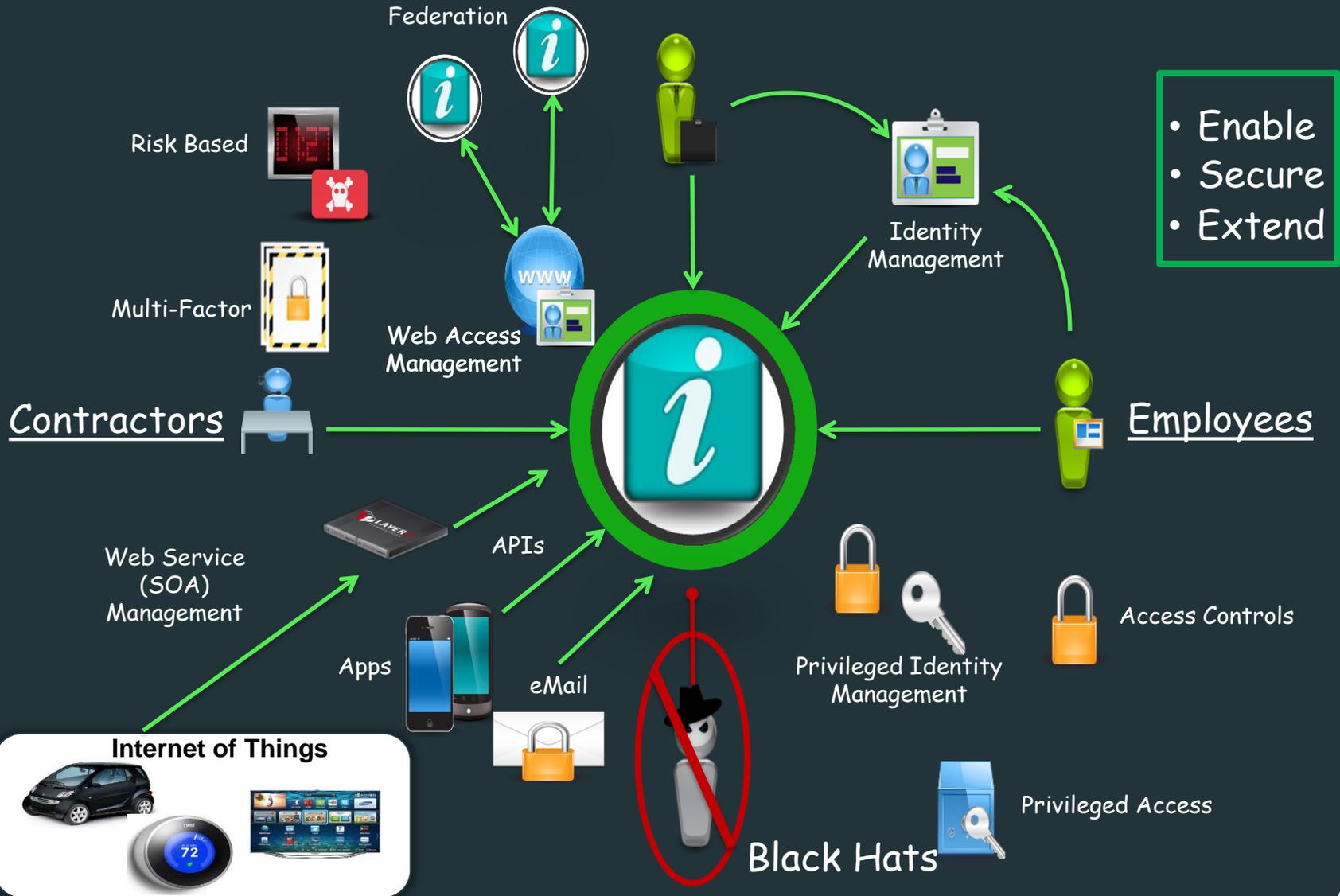
# Citizens



# Citizens



# Citizens



# Citizens

CA SSO

CA Identity Suite\*

CA Identity Governance

CA Directory

CA Risk Authentication\*\*

Risk Based

CA Advanced Authentication\*\*

Multi-Factor

Contractors

CA API Gateway

Web Service (SOA) Management

Apps

Internet of Things

APIs

eMail

CA EMM\*\*

Identity Management

Employees

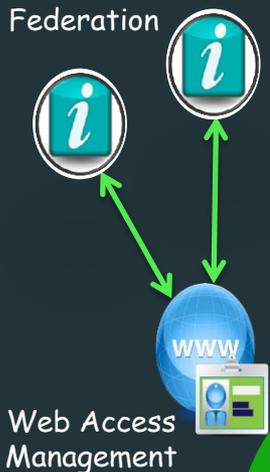
Privileged Identity Management

Access Controls

CA Privileged Identity Management

Privileged Access

Black Hats





Leveraging  
Privileged Identity  
Governance to  
Improve Security  
Posture

# Our System Administrators are the Good Guys

“We only have a few privileged users”

“They are background checked”

“Our SysAdmins are the Good Guys”

“We don’t allow shared account access  
(do we?)”



Proprietary information; for internal use only.

No unauthorized use, copying or distribution.

# Target - Was a BIG target and so was...

**SONY**

**“Cyber Attack on Sony Pictures is Much More than a Data Breach”**

-InfoSec Institute, 8 Dec 2014

- **Target** – Nov 27<sup>th</sup> – Dec 15<sup>th</sup>, **40 Million** credit and debit card numbers stolen **70 million** – Customer records including name, address, email address and phone number. **\$200 Million** estimated cost to credit unions & local banks for reissuing 21.8 million cards — about half of the total stolen.
- **Home Depot** – April – September, **56 Million credit and debit cards compromised**, along with customer’s name, address, email address, and matching that with Date of Birth and SSN allows the bad guys to change the PIN through bank’s automated voice systems
- **UPS** – Jan 20<sup>th</sup> - Aug 11<sup>th</sup>, 51 stores in 24 states (including California), Credit and Debit Card information



# How do these attacks work?



**Step 1** – Identify a device or network of devices running remote desktop software.

**Step 2** – Serve up the malware via a Phising email, or “drive-by-download” of an infected web site.

**Step 3** – Now they are inside, leveraging the RDP (remote desktop protocol) to position a memory scraper tool (the POS device) or to wait and capture credentials to leverage access to system administration functions

# “Click” or “Don’t Click”

Junk Messages		68 Messages
From	Subject	Date
<a href="mailto:harwi079dd8@abrahamlee.com">harwi079dd8@abrahamlee.com</a>	Make sure to read this	9/16/2014 7:25 am <a href="#">Deliver</a>
<a href="mailto:jzyrouy@c-corb.com">jzyrouy@c-corb.com</a>	P_E_N.I..S-- E_N_L-A-R_G E_M_E-N..T__-P_I..L L.S. William.harrod	9/16/2014 7:08 am <a href="#">Deliver</a>
<a href="mailto:hsnewswire@newswirepubs.com">hsnewswire@newswirepubs.com</a>	IS recruits Western women   Student visa loopholes   Dutch lessons	9/16/2014 7:01 am <a href="#">Deliver</a>
<a href="mailto:Emily_Truong@mail.vresp.com">Emily_Truong@mail.vresp.com</a>	CONFIRMED SEAT! The New VMware DR/BC at Backup Prices	9/16/2014 6:19 am <a href="#">Deliver</a>
<a href="mailto:subjoinedy54@sociopsychological.in">subjoinedy54@sociopsychological.in</a>	my new photo ;)	9/16/2014 5:17 am <a href="#">Deliver</a>
<a href="mailto:william.harrod27@feelnumb.com">william.harrod27@feelnumb.com</a>	Make sure to read this	9/16/2014 5:03 am <a href="#">Deliver</a>
<a href="mailto:qpdsgffht@aqwr.net">qpdsgffht@aqwr.net</a>	Levtira & Vigara Today ~ SALLE!	9/16/2014 5:02 am <a href="#">Deliver</a>
<a href="mailto:harwi074f@axtel.net">harwi074f@axtel.net</a>	ISM.TO Is Back In Position For A Huge Jump	9/16/2014 3:57 am <a href="#">Deliver</a>
<a href="mailto:featheryh2@sys.sociopsychological.in">featheryh2@sys.sociopsychological.in</a>	my new photo ;)	9/16/2014 3:55 am <a href="#">Deliver</a>
<a href="mailto:william.harrodb1@infoeasy.ch">william.harrodb1@infoeasy.ch</a>	ISM.TO Is Back In Position For A Huge Jump	9/16/2014 3:55 am <a href="#">Deliver</a>
<a href="mailto:harwi07d9bb@oddgraphic.com">harwi07d9bb@oddgraphic.com</a>	Make sure to read this	9/16/2014 3:51 am <a href="#">Deliver</a>
<a href="mailto:william.harrod4c0@pol.ir">william.harrod4c0@pol.ir</a>	Make sure to read this	9/16/2014 3:39 am <a href="#">Deliver</a>
<a href="mailto:harwi07c93@euskaltel.es">harwi07c93@euskaltel.es</a>	ISM.TO Is Back In Position For A Huge Jump	9/16/2014 3:15 am <a href="#">Deliver</a>
<a href="mailto:william.harrodefde@allpackhellas.gr">william.harrodefde@allpackhellas.gr</a>	ISM.TO Is Back In Position For A Huge Jump	9/16/2014 3:09 am <a href="#">Deliver</a>
<a href="mailto:wgrlyhmjxf@tqq.org">wgrlyhmjxf@tqq.org</a>	Purchaase Vigara --59% Off!	9/15/2014 10:48 pm <a href="#">Deliver</a>
<a href="mailto:yhfcqloi@tlmfxe.net">yhfcqloi@tlmfxe.net</a>	Puurchase Levtira & Viigara Now -- 0.69\$	9/15/2014 10:19 pm <a href="#">Deliver</a>
<a href="mailto:fekwaecwhj@cul.org">fekwaecwhj@cul.org</a>	Buy Levtiira + Vigara Tooday -- 0.71\$ --63% Off!	9/15/2014 8:17 pm <a href="#">Deliver</a>
<a href="mailto:Newsletter@ndia.org">Newsletter@ndia.org</a>	=?windows-1252?Q?NDIA_-S&ET_Breakfast_-Under_Secretary_for_S&T_to_Speak?=-	9/15/2014 7:07 pm <a href="#">Deliver</a>
<a href="mailto:info@mail.scmagazineus.com">info@mail.scmagazineus.com</a>	Reducing Cyber Risk in Industrial Control Systems with Advanced Network Segmentation	9/15/2014 6:11 pm <a href="#">Deliver</a>
<a href="mailto:Jen.Johnson@vetfed.com">Jen.Johnson@vetfed.com</a>	[Itsccl_membership] IT SCC Biweekly Update: September 15-29	9/15/2014 5:57 pm <a href="#">Deliver</a>
<a href="mailto:galina.glebova@investgold.co.za">galina.glebova@investgold.co.za</a>	The only method to recharge your loving life	9/15/2014 5:55 pm <a href="#">Deliver</a>
<a href="mailto:pab5@cox.net">pab5@cox.net</a>	Prayer Request - CORRECTION	9/15/2014 5:53 pm <a href="#">Deliver</a>
<a href="mailto:harwi071fc@ucuzdekorasyon.org">harwi071fc@ucuzdekorasyon.org</a>	The Race Is On!	9/15/2014 4:47 pm <a href="#">Deliver</a>

# “Click” or “Don’t Click”

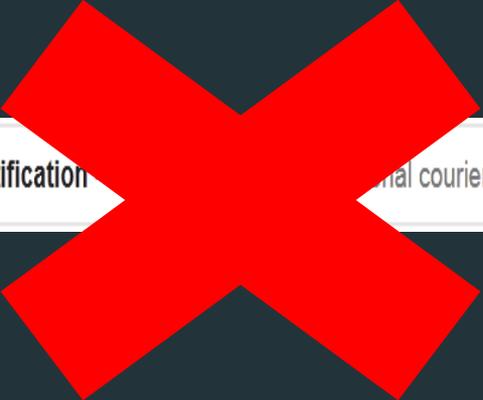
   **TNT Express**

**Delivery Notification - TNT e x p r e s s** International courier delivery services company Delivery Notification Courier

**Sep 16**

# “Click” or “Don’t Click”

**TNT Express**      **Delivery Notification**      ...nal courier delivery services company Delivery Notification Courier      **Sep 16**



# “Click” or “Don’t Click”



**Mr. Francis Bolton**

**PAYMENT OF YOUR OVER DUE FUND THROUGH ATM CARD** - Hello Now we have arranged your payment of (\$:

# “Click” or “Don’t Click”



**Mr. Francis Bolton**      **PAYMENT OF YOUR O**      **GH ATM CARD** - Hello Now we have arranged your payment of (\$:

# “Click” or “Don’t Click”

   | Virginia

My Pictures for you

# “Click” or “Don’t Click”



# What does this have to do with my Agency – Why do I care?

**176**

**Million**  
Government/Military records exposed  
Jan – June 2014

**\$4.4M**

is the average cost of a security breach



Sources: Insurance Networking News/Ponemon, *The Cost of a Data Breach Versus the Cost of More Security*, July 2013

VentureBeat, *[redacted] CIO leaves in wake of security breach as chip cards move in*, March 2014

Forbes.com, *[redacted] CEO [redacted] Resigns In Data Breach Fallout*, May 2014

Yahoo, *Data-breach costs take toll on [redacted] profit*, Feb 2014

© 2015 CA. All rights reserved. CA confidential and proprietary information; for internal use only.  
No unauthorized use, copying or distribution.

# Who are insiders and what are the threats?

## Types of Insiders



**Malicious Insiders**



**Exploited Insiders**



**Careless Insiders**

## Types of Threats



# The Challenge of Privileged Identities and Access



All- Powerful Access

Unrestricted Root or Super-User Access  
Lack of Segregation of Duties Enforcement  
Abuse, Intentional, or Inadvertent  
Service Accounts, Scripts, Cron Jobs



Lack of Accountability

Lack of a Strong Audit Trail  
Who did What - Finger-pointing  
Use of Shared Accounts  
Able to stop Logging and Services

The business value of Privileged Identity Governance is that it addresses the challenges of all-powerful access and lack of accountability by automating the relationship between trusted people, their credentials, and their access rights across the enterprise.

# Privileged Identity Governance



**Privileged Identity Governance brings together three critical areas, so agencies can remove common exploitation points within their IT environments and prevent insider and external attacks:**

**Identity and access governance**

**Privileged identity management**

**User activity reporting**

# Identity and access governance



- ✓ Leverage analytics to assess, audit, and clean up excessive access rights
- ✓ Automate entitlements, roles, and periodic certification of users
- ✓ Enforce consistent and centralized policies for access and Segregation of Duties (SoD)
- ✓ Monitor and report on who has access to what, and who approved that access

# Privileged identity management

- ✓ Leverage fine-grained access controls & implement least privilege access
- ✓ Automate access to Root, Super-User, and Escalated Privileges via a password check-out process
- ✓ Enforce role appropriate command validation
- ✓ Provide “break-glass” capability for exigent circumstances with appropriate compliance checking



# User activity reporting

## User Certification Report

### Role for Ellis Howard

	Role	Details
✓	Employee	On 10/17/2012 01:20:17 PM Michael Allen Approved
✓	Executive	On 10/17/2012 01:20:17 PM Michael Allen Approved

### Entitlements for Ellis Howard

	Entitlement	Details
✓	Domain Users Domain Users, ForwardInC-AD2K3, WinNT	On 10/17/2012 01:20:17 PM Michael Allen Approved
✓	employees employees, Internal-HelpDesk, ServiceDesk	On 10/17/2012 01:20:17 PM Michael Allen Approved
✓	expenses expenses, SAPr3-PROD, SAP	On 10/17/2012 01:20:17 PM Michael Allen Approved
✓	mailbox mailbox, ForwardInC-EX2k3, Exchange	On 10/17/2012 01:20:17 PM Michael Allen Approved
✓	SelfServiceApp SelfServiceApp, SAPr3-PROD, SAP	On 10/17/2012 01:20:17 PM Michael Allen Approved

User: Marge Walton, walma01

### Role for Marge Walton

	Role	Details
✗	Customer Service - non managers	On 10/17/2012 01:21:27 PM Michael Allen Rejected
✓	Employee	On 10/17/2012 01:22:09 PM Michael Allen Approved
✓	Executive	On 10/17/2012 01:22:09 PM Michael Allen Approved
✓	Manager	On 10/17/2012 01:22:09 PM Michael Allen Approved
✓	Procurement Department	On 10/17/2012 01:22:09 PM Michael Allen Approved

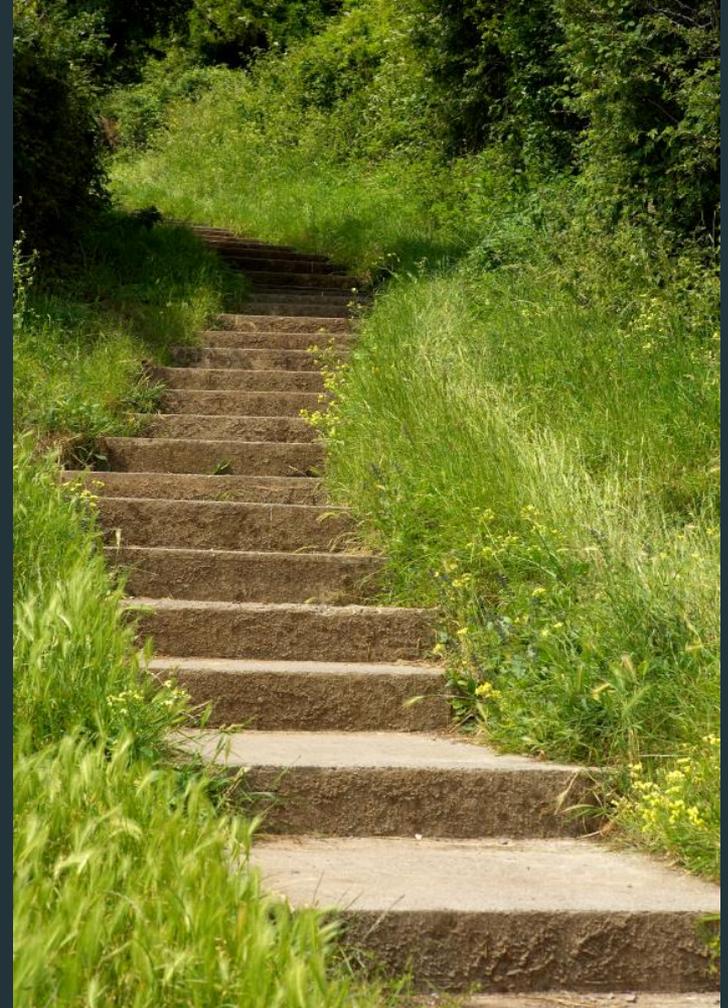
### Entitlements for Marge Walton

	Entitlement	Details
✓	Domain Users Domain Users, ForwardInC-AD2K3, WinNT	On 10/17/2012 01:22:09 PM Michael Allen Approved
✓	employees employees, Internal-HelpDesk, ServiceDesk	On 10/17/2012 01:22:09 PM Michael Allen Approved
✓	Executive_Group Executive_Group, ITServiceDirectory8, Novell	On 10/17/2012 01:22:09 PM Michael Allen Approved
✓	expenses expenses, SAPr3-PROD, SAP	On 10/17/2012 01:22:09 PM Michael Allen Approved
✓	mailbox mailbox, ForwardInC-EX2k3, Exchange	On 10/17/2012 01:22:09 PM Michael Allen Approved
✓	SelfServiceApp SelfServiceApp, SAPr3-PROD, SAP	On 10/17/2012 01:22:09 PM Michael Allen Approved

- ✓ Report on who has access to what, and what they did with that access
- ✓ Certify users have the access they need, and nothing more
- ✓ Enforce account inactivity clean-up, and minimize “role creep”
- ✓ Provide Session recording for system admins and privileged activities

# Next Steps & Best Practices

- ✓ Analyze accounts, entitlements, accesses & Clean-up Orphan Accounts and excessive privileges
- ✓ Identify who needs access to what, build an initial role model starting with privileged users
- ✓ Automate Root, Super User, and Admin password management
- ✓ Enforce Segregation of Duties and provide a Break Glass capability
- ✓ Optimize model and refine



# Questions?





William (Bill) Harrod  
Advisor, Public Sector Security Practice  
[Willam.Harrod@ca.com](mailto:Willam.Harrod@ca.com)





# Archer

**Mark Martens**

**Ed Miller**

Information Assurance Specialists

ISOAG

June 3<sup>rd</sup>, 2015



## Archer Push

- We're going to start pushing more "actionable" reports and items to Archer users
- You will periodically get an email from commonwealthsecurity with a link to an Archer report or item that may require your attention.



# Archer Email for Quarterly Update

1. Please login to Archer using VPN and your RSA SecureID.
2. Click on the link below. The link is to the Quarterly Update report listing all Open Findings that CSRM is tracking for your agency.
  - <https://ITGRCS.vita.virginia.gov/default.aspx?requestUrl=..%2fSearchContent%2fSearch.aspx%3fView%3dReport%26reportId%3d4613%26moduleId%3d167>
3. Export the report to **CSV** format, select the option to "**Exclude all HTML formatting tags**"
4. Open the CSV file using Excel
5. Review each row of findings and update the following columns:
  - Column M: Qtr Date Applied:** ENTER 3/31/YYYY for 1st Quarter of the CY  
6/30/YYYY for 2nd Quarter of the CY  
9/30/YYYY for 3rd Quarter of the CY  
12/31/YYYY for 4th Quarter of the CY
  - Column N: Remediation Response Update:** Enter any changes, updates, or modifications to the remediation for this finding that occurred in the most recently completed quarter.
  - Column O: Revised Expected Due Date:** If the Expected Due Date for the finding has changed, enter it here (MM/DD/YYYY format)
  - Column P: Revised Responsible Party:** If the person responsible for managing or completed the remediation has changed, please enter it here.
6. Save the Quarterly Update CSV file (you may save the file in CSV format)
7. Send the completed Quarterly Update CSV to CSRM by emailing it to: [commonwealthsecurity@vita.virginia.gov](mailto:commonwealthsecurity@vita.virginia.gov)



# Quarterly Update Report

**Findings** ? X

New Modify Save Reports Delete
1 to 3 (of 3)
Refresh Export Print Email

## COV:Quarterly Update Report

Agency x

Agency ▲ 1	Finding ID ▲ 2	Agency Finding Reference Field	Agency Submit Date	Name	Finding	Remediation Overview	Initial Planned Due Date	Expect Due D
[-] Agency: Test Agency								
<a href="#">Test Agency</a>	<a href="#">FND-1748</a>	1	4/4/2014	Batman has too much Control	Separation of duties. Batman is the Risk Manager, ISO, Security Manager, Penetration Tester, data owner, business owner, system owner, developer, and internal auditor for this sensitive system.		4/4/2015	
<a href="#">Test Agency</a>	<a href="#">FND-1749</a>	2	4/4/2014	Baseline Configuration	System baseline is not currently configured per agency standards		4/4/2015	
<a href="#">Test Agency</a>	<a href="#">FND-1750</a>	3	4/4/2014	Media Protection	Disk array storage for mediat is not encrypted		4/4/2015	



# Archer Email for Audit Plan Update

1. Please review the Audit Plan on the link below. This is the most recently submitted audit plan for your agency. You must use your VPN login with your RSA SecureID before you click the link.

<https://ITGRCS.vita.virginia.gov/default.aspx?requestUrl=..%2fSearchContent%2fSearch.aspx%3fView%3dReport%26reportId%3d4614%26moduleId%3d373>

Note the fields "Date Audit Plan Submitted" and "Date Audit Plan Expires" on the report. Ensure that you send an updated Plan to CSRM by the expiration date. If changes to your plan occur at any time, please send us an update.



# IT Security Audit Plan

## IT Security Audits



1 to 1 (of 1)



### COV:Audit Plan TEST

Options

Drag a column name here to group the items by the values within that column.

Agency ▲ 1	Audit Plan ID ▲ 2	Date Audit Plan Submitted	Date Audit Plan Expires	Number of Audits Past Due	Most Current AP
<u>Test Agency</u>	<u>AP-228973</u>	5/27/2015	5/27/2016	0	Yes
IT Systems Scheduled to Audit	Scheduled Audit Description	Scheduled Audit Completion	Actual Audit Completion	Domain Audit	Domain Audit Family
<u>Fake Sensitive System</u>	This is a fake audit of a fake system, focusing on some real important security controls from SEC501-09.	3/28/2016		No	
<u>All Your Password Are Belong To Us</u>	This fake audit will look at the fake system to assess its compliance with some very real security controls in SEC501-09.	3/23/2016		No	
<u>All Your Password Are Belong To Us</u>	Fake Audit to be performed against fake system to ensure compliance with SEC501-08	10/10/2013	10/10/2013	No	
<u>Fake Sensitive System</u>	Fake audit of Fake Sensitive System to check for compliance against SEC501-08	5/27/2012	5/28/2012	No	



## Export Reports

- You should export reports to the format of your choosing, or in some cases, to the format that CSRM specifies.
- If needed, modify the exported file, and email it back to commonwealthsecurity



# Dashboard View

IT Security Audit Dashboard

Welcome, Joe User

## Agency Datapoints

Agency Name ▲	ISO Certification Status	Audit Plan Status	Current Year Percentage of Audits Received	Current Year Percentage of Quarterly Updates Received	3 Year Audit Obligation	Risk Assessment Plan Status	3 Year Risk Assessment Obligation
<u>Test Agency</u>	<span style="color: red;">●</span>	<span style="color: green;">●</span>	N/A	50%	50%		0%

## Actionable IT Security Audit Information

COV: Scheduled IT Security Audit Issues

No Records Found

## Agency Applications





# Applications



## Enterprise Governance Risk and Compliance

Agency Workspace

### Applications

- New
- Modify
- Save
- Reports
- Delete

1 to 2 (of 2)

Search Results					
Drag a column name here to group the items by the values within that column.					
Application ID	Application Name ▲	Description	Criticality Rating	Count of Critical Business Functions	Last IT Security Audit
APPID-228982	<u>All Your Password Are Belong To Us</u>	This fake application hosts all the agency's encrypted passwords.	Not Rated	0	10/10/2013
APPID-228974	<u>Fake Sensitive System</u>	This is a Fake Sensitive System. It handles credit card data belonging to thousands of fake people. The data is encrypted but there are concerns that there isn't proper network segmentation to separate the PCI network from the rest of Test Agency's fake network.	Not Rated	0	5/28/2012

Page 1 of 1 (2 records)



# Application Information

## Applications: All Your Password Are Belong To Us



Record 1 of 2

First Published: 5/28/2015 10:45 AM Last Updated: 5/28/2015 11:08 AM

### About

### General Information

Agency:	<a href="#">Test Agency</a>	Agency Number:	99,999
Application Name:	All Your Password Are Belong To Us	Application ID:	APPID-228982
Last Updated:	5/28/2015 11:08 AM	Application Type:	
Description:	This fake application hosts all the agency's encrypted passwords.		
Recovery Time Objective (RTO):		IT Security Audits (IT Systems Scheduled to Audit):	<a href="#">SA-228983</a> <a href="#">SA-228984</a>
Customer Impacting:	No	Recovery Point Objective (RPO):	
Sensitive System:	Yes	Customer Impacting Information:	
		Vital Business Function:	



# Scheduled Audit

IT Security Audits: SA-228983



First Published: 5/28/2015 10:46 AM Last Updated: 5/28/2015 10:47 AM

## General Information

IT Systems Scheduled to Audit:	<a href="#">All Your Password Are Belong To Us</a>	Scheduled Audit Tracking ID:	SA-228983
IT Security Audit Plans Reference(s):	<a href="#">AP-228973</a>	Scheduled Audit Description:	This fake audit will look at the fake system to assess its compliance with some very real security controls in SEC501-09.
Scheduled Audit Completion:	3/23/2016	Actual Audit Completion:	
All Audits Complete:	No	CSRM Review Status:	Approved
Planned Auditor:	Umbrella Corporation	Areas for Special Emphasis:	
Domain Audit:	No		

## IT Security Audits

Security Audit Tracking ID	Audit Complete	Date Submitted	Date Approved	CSRM Approval
No Records Found				



# Audit Plan

## Security Audits: AP-228973



First Published: 5/27/2015 2:10 PM Last Updated: 5/27/2015 2:10 PM

### General Information

Agency:	<a href="#">Test Agency</a>	Audit Plan ID:	AP-228973
Date Audit Plan Submitted:	5/27/2015	Date Audit Plan Approved:	5/27/2015
3 Year Period Start Date:	5/27/2015	Countdown to Expiration:	364 Days Remaining
Number of Audits Past Due:	0	CSRM Approval:	Approved
3 Year Period End:	2017		

### Audit Plan Attachment

Name	Size	Type	Upload Date
No Records Found			

### ▼ Scheduled IT Security Audits

Scheduled Audit Tracking ID	IT Systems Scheduled to Audit	Scheduled Audit Description	Scheduled Audit Completion	Actual Audit Completion	All Audits Complete
<a href="#">SA-228981</a>	<a href="#">Fake Sensitive System</a>	This is a fake audit of a fake system, focusing on some real important security controls from SEC501-09.	3/28/2016		No
<a href="#">SA-228983</a>	<a href="#">All Your Password Are Belong</a>	This fake audit will look at the	3/23/2016		No



# Scheduled Audits

## ▼ Scheduled IT Security Audits

Scheduled Audit Tracking ID	IT Systems Scheduled to Audit	Scheduled Audit Description	Scheduled Audit Completion	Actual Audit Completion
<a href="#"><u>SA-228981</u></a>	<a href="#"><u>Fake Sensitive System</u></a>	This is a fake audit of a fake system, focusing on some real important security controls from SEC501-09.	3/28/2016	
<a href="#"><u>SA-228983</u></a>	<a href="#"><u>All Your Password Are Belong To Us</u></a>	This fake audit will look at the fake system to assess its compliance with some very real security controls in SEC501-09.	3/23/2016	
<a href="#"><u>SA-228984</u></a>	<a href="#"><u>All Your Password Are Belong To Us</u></a>	Fake Audit to be performed against fake system to ensure compliance with SEC501-08	10/10/2013	10/10/2013
<a href="#"><u>SA-228986</u></a>	<a href="#"><u>Fake Sensitive System</u></a>	Fake audit of Fake Sensitive System to check for compliance against SEC501-08	5/27/2012	5/28/2012



# Completed Audit

## IT Security Audits: SA-228984



First Published: 5/28/2015 11:03 AM Last Updated: 5/28/2015 11:21 AM

### General Information

IT Systems Scheduled to Audit:	<u>All Your Password Are Belong To Us</u>	Scheduled Audit Tracking ID:	SA-228984
IT Security Audit Plans Reference(s):	<u>AP-228973</u>	Scheduled Audit Description:	Fake Audit to SEC501-08
Scheduled Audit Completion:	10/10/2013	Actual Audit Completion:	10/10/2013
All Audits Complete:	Yes	CSRM Review Status:	Approved
Planned Auditor:	Umbrella Corporation	Areas for Special Emphasis:	
Domain Audit:	No		

### ▼ IT Security Audits

Security Audit Tracking ID	Audit Complete	Date Submitted	Date Approved
<u>SECAUD-228987</u>	Yes	5/27/2012	5/27/2012



# Finding

## General Information

Security Audit Tracking ID:	SECAUD-228987	Scheduled IT Security Audits Reference(s):	<a href="#">SA-228984</a>
Date Submitted:	5/27/2012	Audit Complete:	Yes
Date Approved:	5/27/2012	CSRM Approval:	Approved
Alternative Application Name:			

## Findings (IT Security Audit Findings)

Finding ID	Agency	Agency Finding Reference Field	Finding	Affected Applications
<a href="#">END-1748</a>	<a href="#">Test Agency</a>		Separation of duties. Batman is the Risk Manager, ISO, Security Manager, Penetration Tester, data owner, business owner, system owner, developer, and internal auditor for this sensitive system.	<a href="#">All Your Password Are Belong To Us</a>



# Finding Continued

## Findings: FND-1748



Response Workflow and Description

### Remediation

Remediation Overview:			
Initial Planned Due Date:	4/4/2015	Type:	
Actual Remediation Start Date:		Actual Remediation Date:	
Responsible Person(s):	Batman	Remediation Status:	Not Started

### Remediation Response Updates

Quarter Date Applied ▲	Remediation Response Update	Revised Expected Due I
No Records Found		

### Corrective Action Plans

Name	Estimated Completion Date	Actual C
<u>TEST CAP</u>		



# CAP

## Remediation Plans: TEST CAP



### ▼ General Information

Agency:	<u>Test Agency</u>	Remediation Plan ID:	RP-160
Name:	TEST CAP	Applied Date:	10/10/2014
Description:	This Test CAP covers the audits for APABT and FSS.		
Estimated Cost:	\$ 0.00	Actual Cost:	\$ 0.00
Estimated Start Date:	5/28/2015	Actual Start Date:	5/28/2015
Initial Estimated Completion Date:	5/28/2015	Actual Completion Date:	
Estimated Completion Date:		Days Open:	231
Type:	Control	Status:	Closed

### ▼ Quarterly Update Information

Quarterly Updates Due - Current Year:	4	Quarterly Updates Due - Previous Year:	0
Quarterly Updates Submitted - Current Year:	2	Quarterly Updates Submitted - Previous Year:	0



# CAP Continued

## Remediation Plans: TEST CAP



### ▼ Quarterly Updates

	Remediation Plan Status	Date Quarterly Update Applied	Date Quarterly Update Sub
<a href="#">View</a>	Completed	1/1/2015	1/1/2015
<a href="#">View</a>		6/1/2015	5/1/2015

### ▼ Related Findings

Finding ID	Agency	Agency Finding Reference Field	Finding	Status	Expected Due Date	Initial Planned Due Date	Actual Remediation Date
<a href="#">FND-1747</a>	<a href="#">Test Agency</a>		Witnessed a user attempt to login in 20 times in a row within a 5 minute period and was not locked out. This is concerning because this system contains all the agency's fake passwords.  AC-07  a. Enforces a limit	Closed		5/28/2015	10/10/2013



# Quarterly Update



## Enterprise Governance Risk and Compliance

Preferences R

Agency Workspace

Remediation Plan Quarterly Updates: 228993

 Save
  Apply
  Edit
  Delete

General Information			
Date Quarterly Update Applied:	1/1/2015	Date Quarterly Update Submitted:	1/1/2015
CSRM Approval:	Approved	Remediation Plan Status:	Completed

▼ Quarterly Update Document		
Name	Size	Type
No Records Found		



# Agency Info and Scorecard

## Agency: Test Agency



### ▼ General Information

Agency Name:	Test Agency	Agency Acronym:	TEST
Web Site:		Partnership Full Service Customer:	Yes
Agency Number:	99999	Number of Employees:	0
Agency Secretariat:	Locality	Government Branch:	Locality
Annual Report Governance (subject to):	Yes		
Agency Size (Group):	I	CSRM Analyst:	Mark Ma
Description:	This is a Test Agency for Demonstration purposes		

### ▼ Agency Scorecard Data

ISO Certification Status:	<span style="color: red;">●</span>	Previous Year ISO Certification Status:	<span style="color: green;">●</span>
3 Year Audit Obligation:	50%	3 Year Audit Obligation - Previous Year:	100%
Audit Plan Status:	<span style="color: green;">●</span>	Audit Plan Status - Previous Year:	<span style="color: green;">●</span>



Virginia Information Technologies Agency

# Upcoming Events





## 2015 Conference

RVAssec is the first Richmond, Virginia, security convention to bring top speakers to the mid-atlantic region. The 2015 conference will be held on Thursday, June 4th and Friday June 5th at the Commonwealth Ballroom at VCU's University Commons. Training classes will be held on Wednesday, June 3rd.

Keynotes:

G. Mark Hardy - Founder of CardKill

Jennifer Steffens - IOActive CEO

Virginia Governor Terry McAuliffe

More information can be found at: <http://rvasec.com/>



## IS Orientation

**When: Thursday, June 16th, 2015**

**Time: 1:00 pm to 3:00 pm**

**Where: CESC , Room 1211**

**Register here:**

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



## Future ISOAG

**July 1, 1:00 - 4:00 pm @ CESC**

**Speaker: Tommy Johnstone, Office of Attorney General**

**ISOAG meets the 1<sup>st</sup> 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](mailto:CommonwealthSecurity@VITA.Virginia.Gov)**



**ADJOURN**

**THANK YOU FOR ATTENDING**

