



Common Knowledge: Kevin Burns

SECURITY IN THE CLOUD

(aka-"Insecurity in the Cloud")



Real Issue:

**You don't know what you don't know
For Instance -**

- First Question – who is responsible for securing what?
- Who has access to what data?
- Which way did it go? (the data that is)
- “You destroyed what data?”
- What technologies are being used?
 - “Who made those firewalls?”
 - “Who configured those firewalls?”



Assessing the vendor

- How likely is the vendor to continue the service?
- How financially stable is the vendor?
- To what extent does the vendor use subcontractors?
- What are the vendor's standard security practices?
- What is the vendor's track record with security?



So What Now?

Getting serious for a minute

- IT STARTS WITH THE CONTRACT!
- Contracts Are The Key Legal Enforcement Mechanism
 - » (BTW - Cloud Security Alliance –great source)
 - Examples – “Right to Audit” clauses
 - “Adherence to compliance” (PCI)
 - How will provider respond to INFO requests?
- Termination of contract handled? (Assets returned)



Legal Stuff – (Cont.)

- Service Level Agreements – necessary performance??
- NIST 800-144 – Security - Public Clouds
- Breach notification process must be defined!!!
- Data allowed/not allowed to be co-mingled
- Contract language stipulates where the data will reside
- Disaster Recovery/Redundancy (other locations of provider)



- **SAS 70 Type II Compliance-** (What the heck is that?...Replaced by SSAE 16 in 2010 – Never mind)

Certifications

- Differences – SAS 70 – verified that controls/processes at data center were followed (cloud providers still touting their SAS 70s even as of this date)
- SSAE 16 – does the above AND also requires verification of design and operating effectiveness. Attestation of system effectiveness versus SAS 70 controls focus
- And look for a recent independent Vulnerability and Penetration test (perimeter network)!!!!



THREATS TO YOUR CLOUD

- Cloud Security Alliance has identified threats to cloud security:
 - Data breaches will continue (duh) - but why? Because they are only as strong as their own security posture (firewall patches)

Threats - Cloud Security

- Data loss – (gulp – pun intended) - the drives went where? Your provider went bankrupt?
- DDOS - (Mass.Gov or e-mail (if ever in the cloud) not accessible?) – Oh oh!
- Malicious insiders (my favorite!) Maybe keep the encryption keys in-house
- Abuse of cloud services – “My cloud provider is serving up malware?”
- Shared technology – “Hey, hey, you you get off of my cloud” (you knew that was coming)



Just Sayin.....

- **Reminder – (so you don't forget)**
- The Cloud Security Alliance calls out **Lack of Due Diligence as a MAJOR threat** Threats -continued
- “Enterprises may push applications that have internal on-premises network security controls into the cloud, where those network security controls don't work. If enterprise architects don't understand the cloud environment, their application designs may not function with proper security when they're run in a cloud setting, the report warned.”

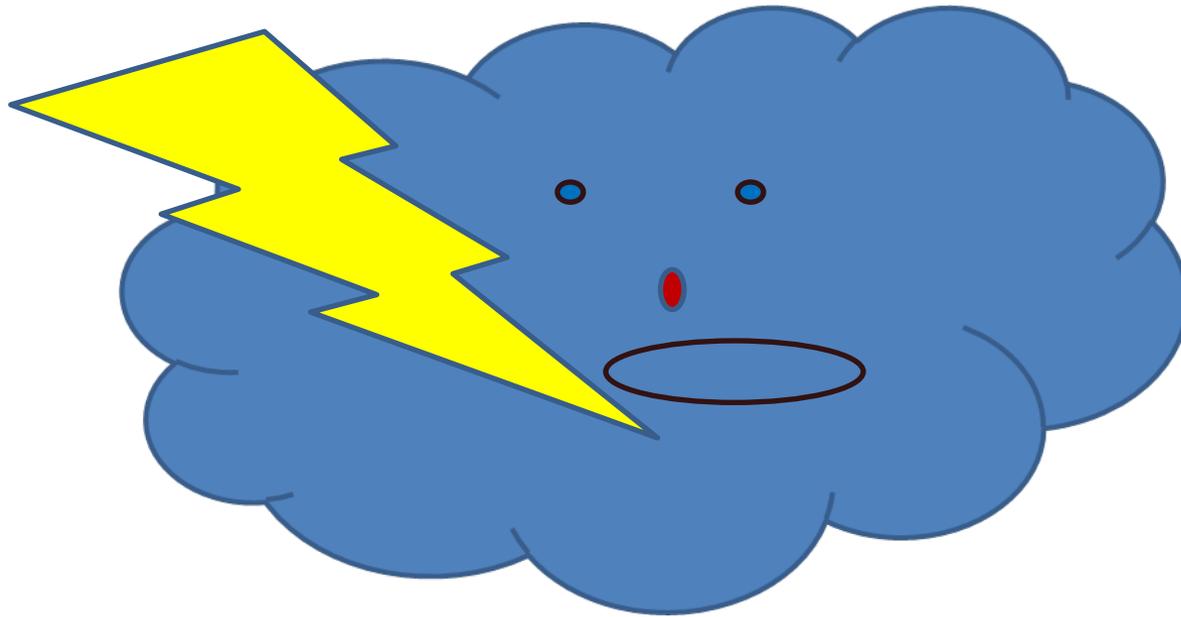


Summary

- Tactics
 - Be Proactive – Insist on communication(s) with CISOs of your cloud security provider.....
- So.....
- Obtain explanations of their security controls – both at a high level & low level
 - Put the data owner on notice that they bear responsibility
 - Insist on accurate data flow & network diagrams - **you cannot protect it if you don't know**: origin, destination, transmission, and storage locations.
 - **THE ABOVE SEEMS OBVIOUS BUT.....**



Any questions?





Identity and Access Management



Massachusetts Office of Information Technology
Executive Office for Administration and Finance

Aldo Pietropaolo (IAM Technical Lead & Industry SME)
MassIT



Agenda

- Identity And Access Management
- Current Cybercrime Landscape
- Addressing The Gaps
- Program Benefits
- Real Examples
- Questions



Identity And Access Management

Give the right people the right access to the right resources and applications, at the right time and for the right reasons.

The screenshot shows a web browser window with the URL <https://iam.state.ma.us>. The page title is "Commonwealth Access Manager" and the subtitle is "Managed access to Commonwealth Applications". The main content area contains a login form with the following elements:

- A heading: "Enter your username and password to access the requested Commonwealth application"
- A "Username" label followed by an input field containing "Enter username" and a small example "(example: jdoe)" below it.
- A "Password" label followed by an input field containing "Enter password".
- A "Login" button.

Below the login form, there is a security notice: "TO SAFEGUARD YOUR LOGON SESSION, PLEASE CLOSE YOUR BROWSER WINDOW AFTER YOU LOGOFF." and a link: "If you do not have access to Commonwealth Access Manager, Please [click here](#) to access the requested page". At the bottom left, the copyright notice reads "© 2012 Commonwealth of Massachusetts".



Cyber-Criminal Attacks Continue To Increase

- Malware attacks targeting **identity theft** are increasing (Examples: Home Depot, Target, Citibank, JP Morgan Chase)
 - State employee and citizen identity and personal data at highest risk.
 - Access to state information systems at risk.
- Increase targeting of mobile devices (Android, Apple)
 - SMS Trojans – Capable of stealing your text messages.
 - Ransom Ware – Capable of locking personal files and asking for ransom.
- Increase in advanced and persistent cyber-crime threats. These operate silently and avert detection until personal information is stolen and put into the black market.
- Increase in exploiting zero day attacks in vendor products.
- State regulatory requirements are becoming more stringent.
 - FBI Criminal Justice, HIPPA, Federal Security Mandates
- Access control cited as one of the most frequent gaps
 - (Deloitte NASCIO Report: http://www.nascio.org/publications/documents/Deloitte-NASCIOCybersecurityStudy_2014.pdf)



Addressing The Gaps

Significantly Reduce Implementation Costs And Address Security Gaps

Provide Faster Deployment And Consistent Security And Audit Capabilities

**IAM Assembly Line
(Continuous Delivery)
(Agile)**



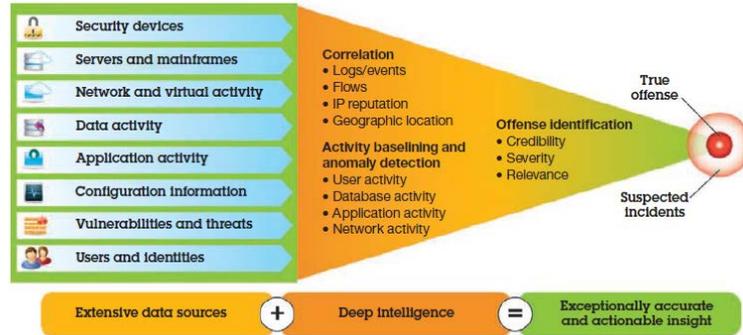
Significantly reduce implementation costs by an estimated 35% – 45%

- By adopting a continuous deployment model, small packages are processed in an assembly line fashion to yield quality results.
- Measurable return on investment for CAPEX and OPEX.
- Commonwealth business requirements and IAM technology roadmap will serve as input to assembly line.

**Increase Security
Safe Guards**



Security Intelligence delivers 360-degree view:



**Audit & Access
Re-Certification
Capabilities**



- Centralized service for knowing who has access to what.
- Access re-certification and revocation process – if a user has access to an application and should not, IAM will remove the access.



IAM Program Benefits

An improved enterprise IAM environment enables these benefits



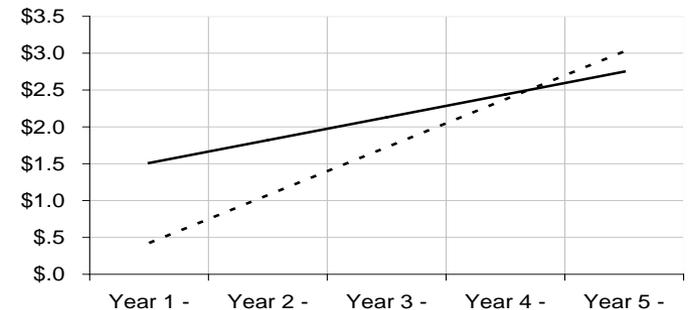
Benefit	Typical Metric
Decreased time to provision accounts	Reduce from weeks to 1h or less
Automated auditing and reporting	Decreased reporting labor through more automated processes
Simplify system architecture	Reduce development costs by 2-5% per system
Standardized login processes that simplify access	Single consolidated login process
Simplify account management & improve accuracy	Reduce labor by 50% or more
Automated password reset function	Reduce help desk calls by 75%+
De-provision accounts quickly	Decrease from days to minutes
Automated provisioning improves accuracy assignment and permissions	Decrease errors by 90% or more
Improved understanding of who has access to speed investigation	Decrease risk
Enforce standardized IAM policies and procedures	Improve compliance, decrease risk
Fewer passwords or other access credentials	Reduce from dozens to a few or one

Which result in a strong, industry demonstrated return on investment



Typical Financial ROI Model

- ROI ranges from 40% to over 100%
- 100% recapture of capital investment in three years or less
- Reduced ongoing operating costs of 20% or greater



———— Total Cost - - - - - Quantifiable Benefits

*Typical Metrics and ROI Model



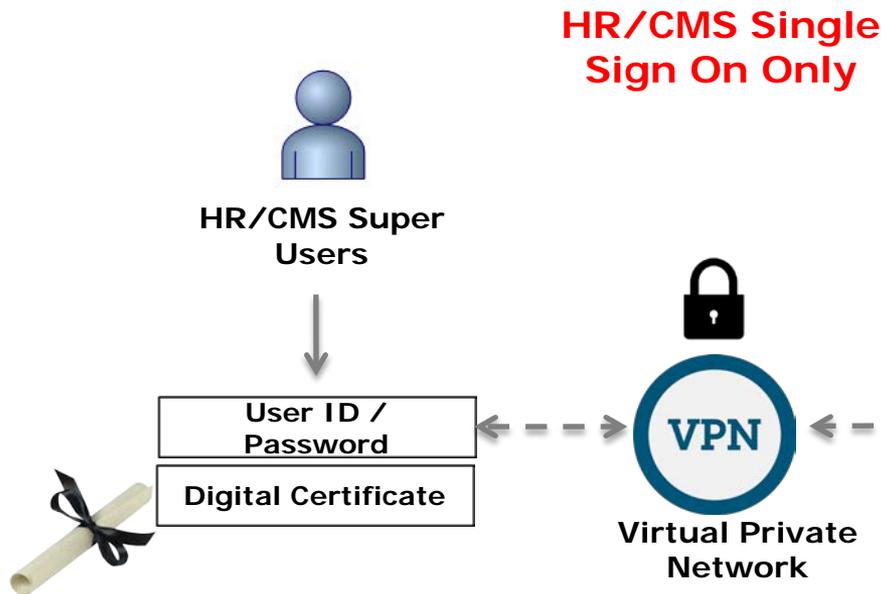
Let's look at some real examples



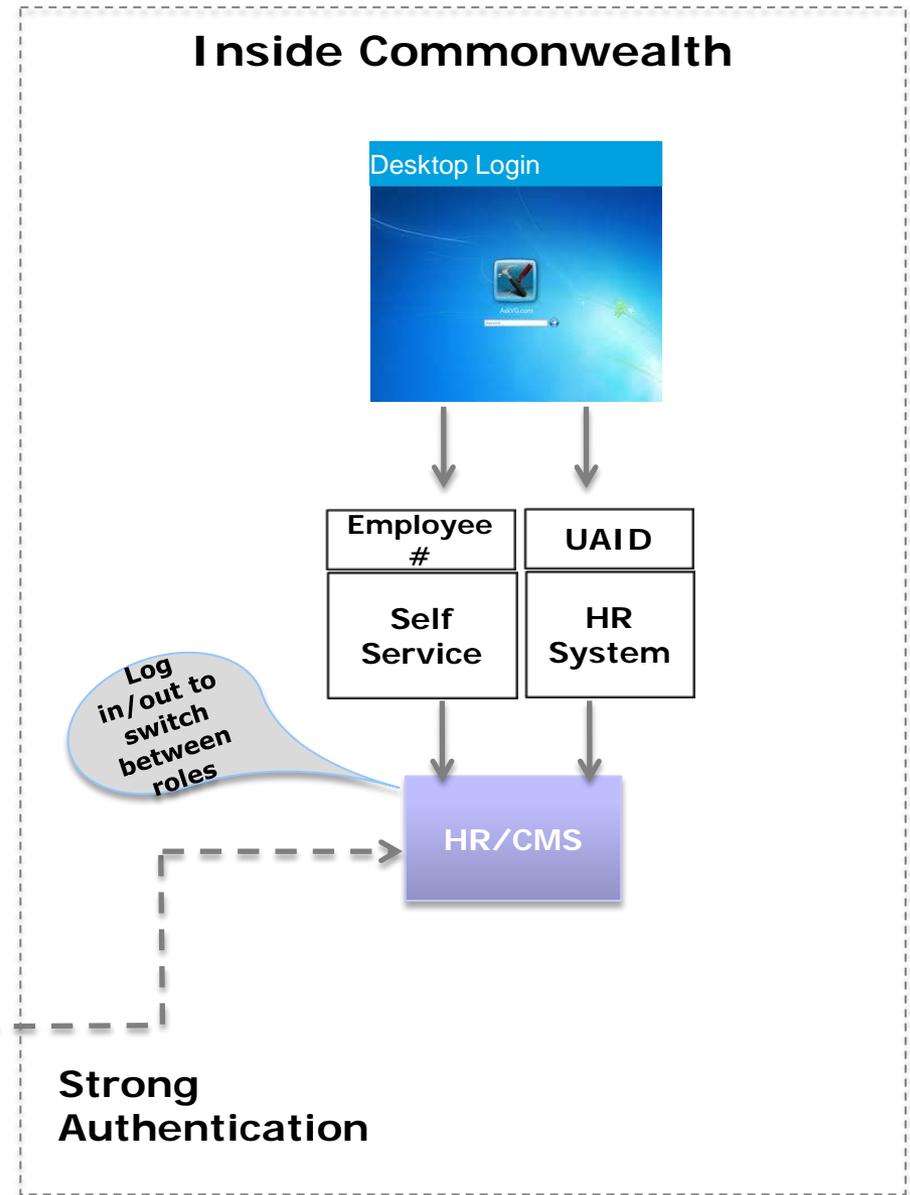
HR/CMS Admin Access Today

Outside Commonwealth (Internet)

- Time And Attendance
- Payroll
- Employee Management
- New Hires
- Employee And Contractor Terminations



Inside Commonwealth



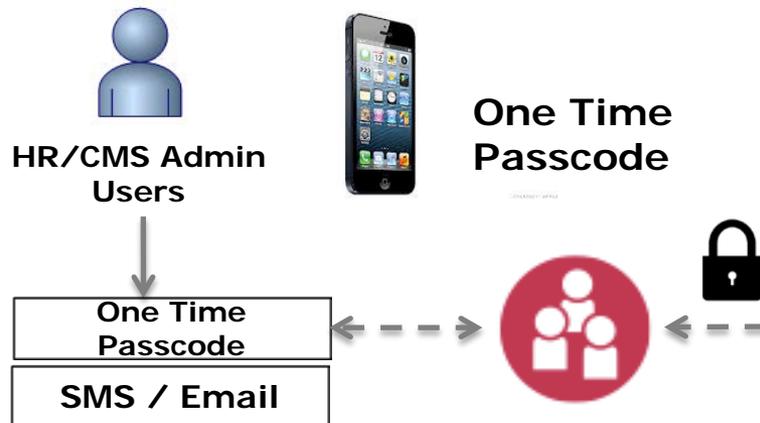


HR/CMS Admin Access Tomorrow

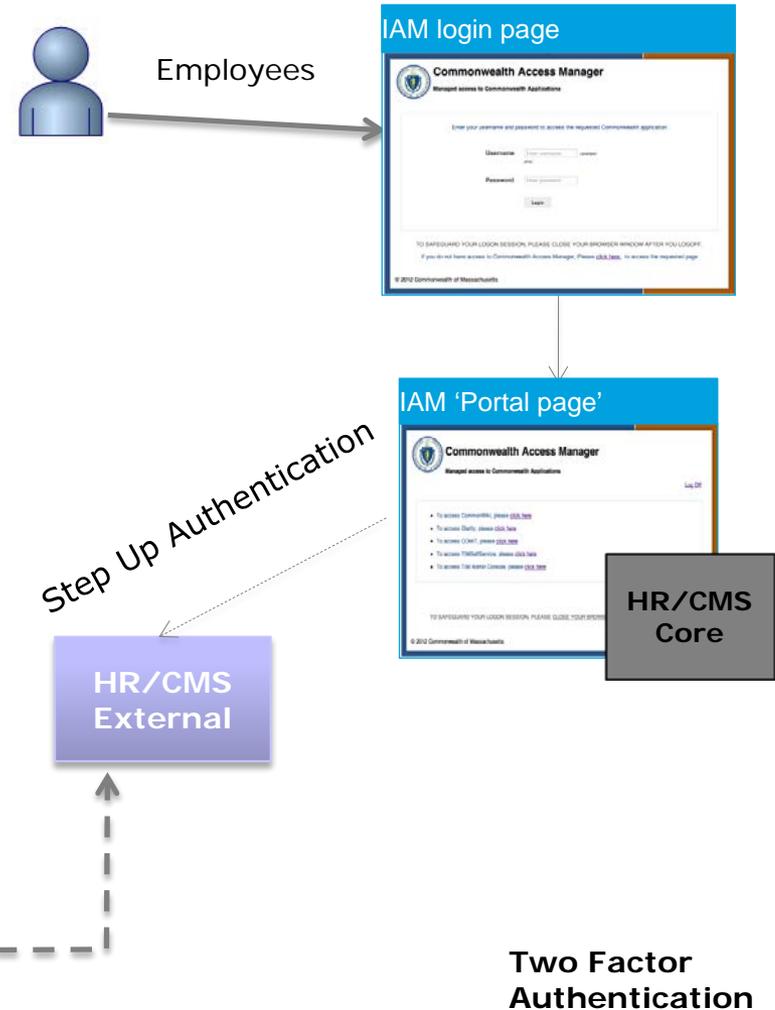
Outside Commonwealth (Internet)

Key Benefits

- Prevent Breaches such as direct deposit bank account modifications.
- Single Sign On to all integrated applications.



Inside Commonwealth

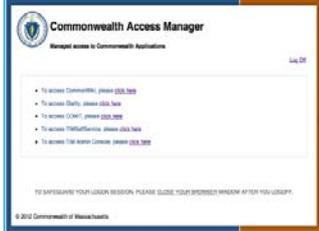




Inter-Agency Cooperation

Agency (MassIT)

Application Landing Page



"JSmith" in MassIT translates to "John.Smith" In DOR, and vice versa for application access.

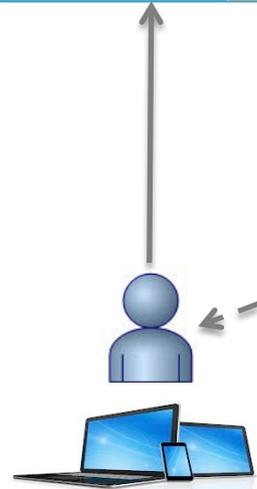
Identity Federation

Identity Federation

Application Landing Page



Single Sign On
To Federated
Agencies



Employee / Contractor in agency **A** has seamless navigation to application(s) in agency **B**. User has Single Sign On for both agencies.



Employee / Contractor in agency **B** has seamless navigation to application(s) in agency **A**. User has Single Sign On for both organizations.



Summary

- Opportunity to realize **ROI** on capital investment within 3 – 5 years, while significantly strengthening Commonwealth security posture and identity management processes
- Increase Inter-Agency Collaboration While Reducing CapEx Costs
 - Use existing systems where applicable for employee, contractor, and citizen access to Commonwealth resources
 - No need to rebuild IAM services that already exist, therefore saving an average of 1.2 – 1.4 Million dollars in CapEx (Industry average for an enterprise IAM foundation)
 - Accelerate common and valuable services to Commonwealth citizens
- Decrease errors **by 80 % – 90 %** which may lead to personal data exposure by introducing a level of continuous automation, service availability, consistency, and quality improvements



Questions?