



INFORMATION SECURITY FORUM
FOR TEXAS GOVERNMENT

IDENTITY ASSURANCE AND DIVERSE USERS

INFORMATION SECURITY FORUM FOR TEXAS GOVERNMENT

RSA

Why are we talking about Identity?

- **Identity has become a primary attack vector.**

Phishing/Spear-Phishing, MITB/MITM attacks, brute force, key logging, social engineering

- Identity lets attackers ‘walk through the front door’ – makes it ‘easy’ to access structured data.
- Identity enables lateral movement for attackers once they are in part of a network. “Credential Harvesting”

“When it comes to massive compromise of an entire network, credentials are a main component. Out of all the incident response engagements that we conducted; 100% of them involved the threat actor compromising valid credentials during the attack.” Chad Holmes, CTO FireEye

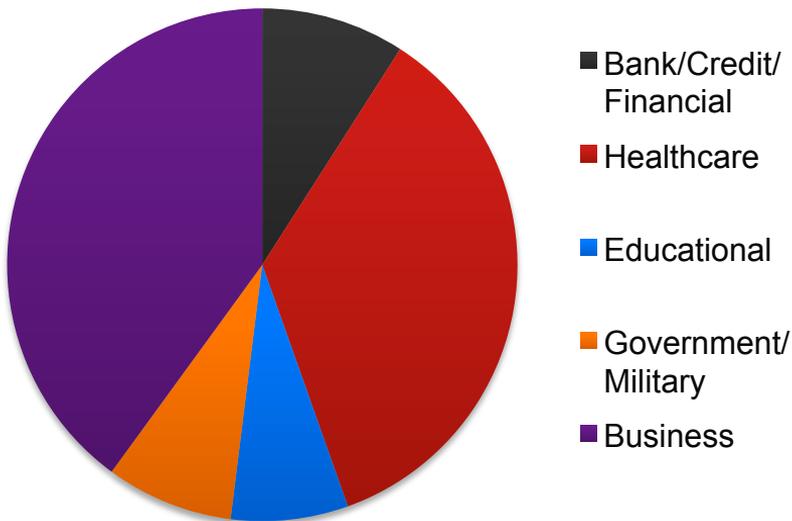
https://www.fireeye.com/blog/executive-perspective/2015/08/malware_lateral_move.html

- Identity information can be used a lot of different ways. (Financial fraud, Healthcare fraud, Data Access)

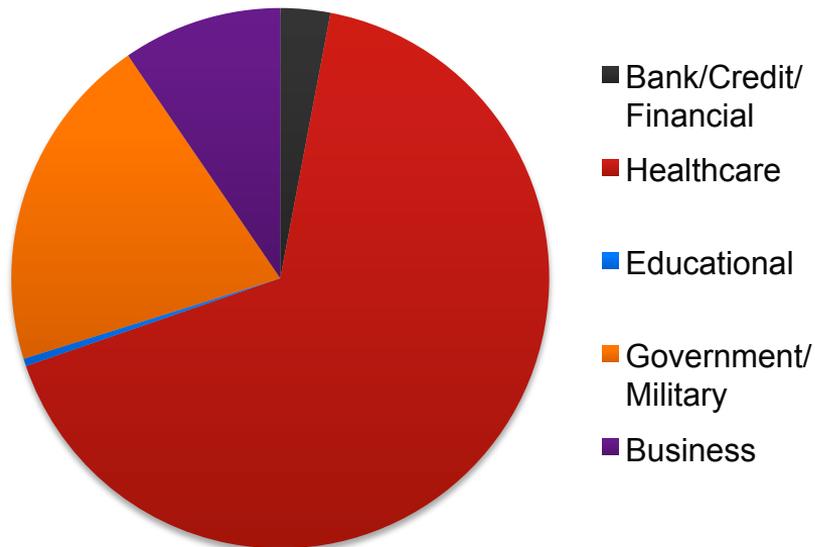
Some Statistics/Stories

- ▶ ID Theft Center - : 781 Breaches, 179M Accounts Compromised in 2015

Breaches

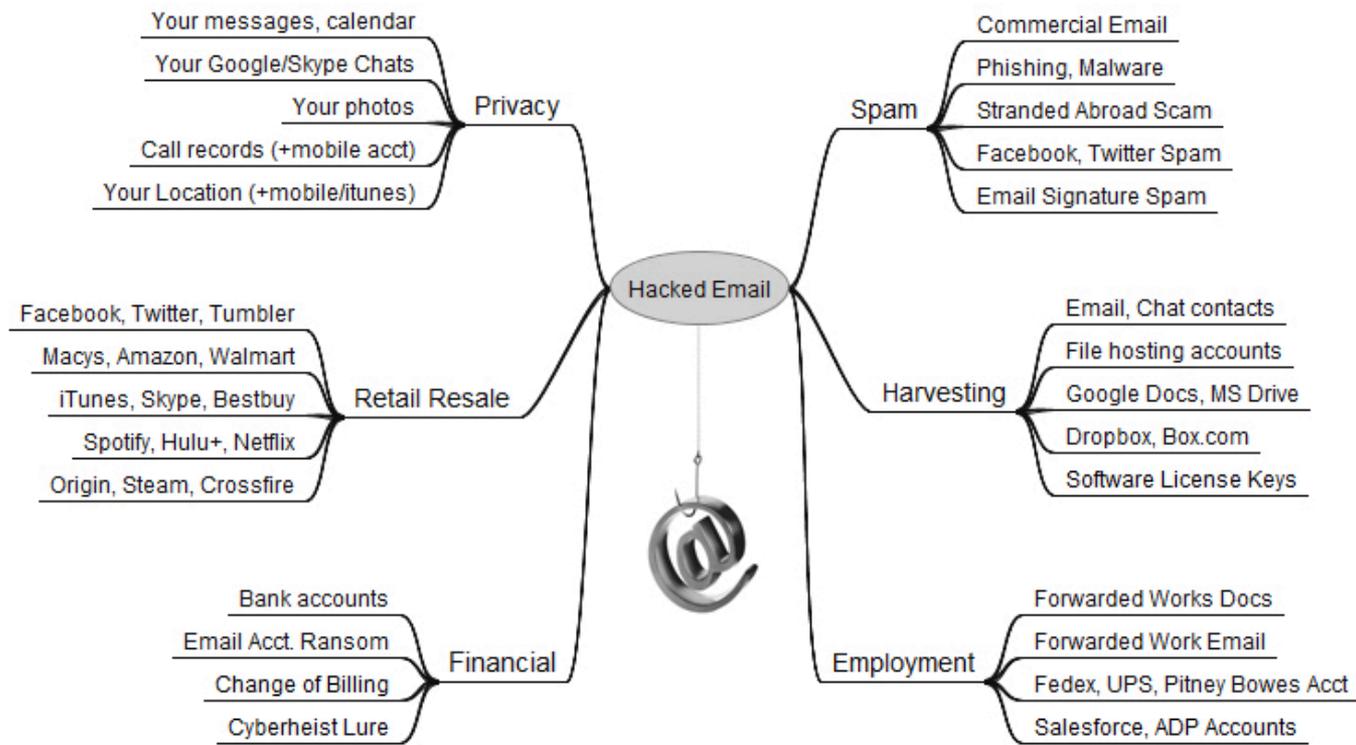


Records



Source: http://www.idtheftcenter.org/images/breach/DataBreachReports_2015.pdf

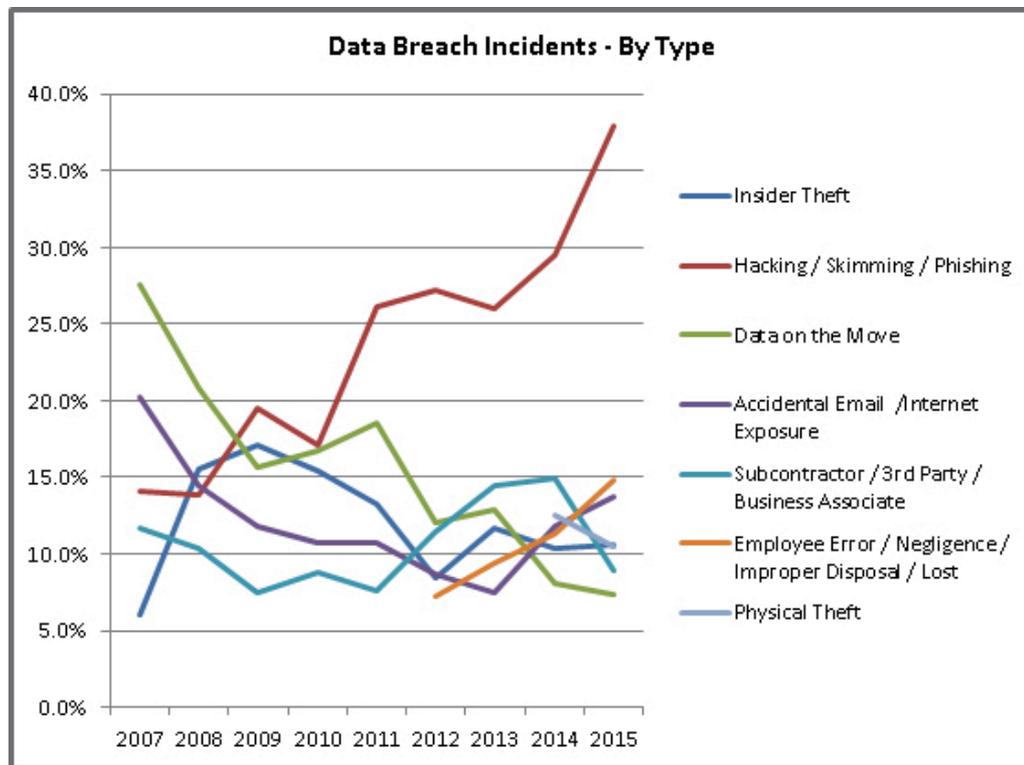
Usages of an E-Mail



Source: <http://krebsonsecurity.com/2013/06/the-value-of-a-hacked-email-account/>

More Stats

While we've gotten better at controlling and securing what we can – what we know about. Hacking has become the primary way that we lose Identity information.



Source: http://www.idtheftcenter.org/images/breach/DataBreachReports_2015.pdf

Balancing Security and Convenience

Usage: Convenient!

Usage: Difficult!



Continuum of Application Security Needs and Approaches

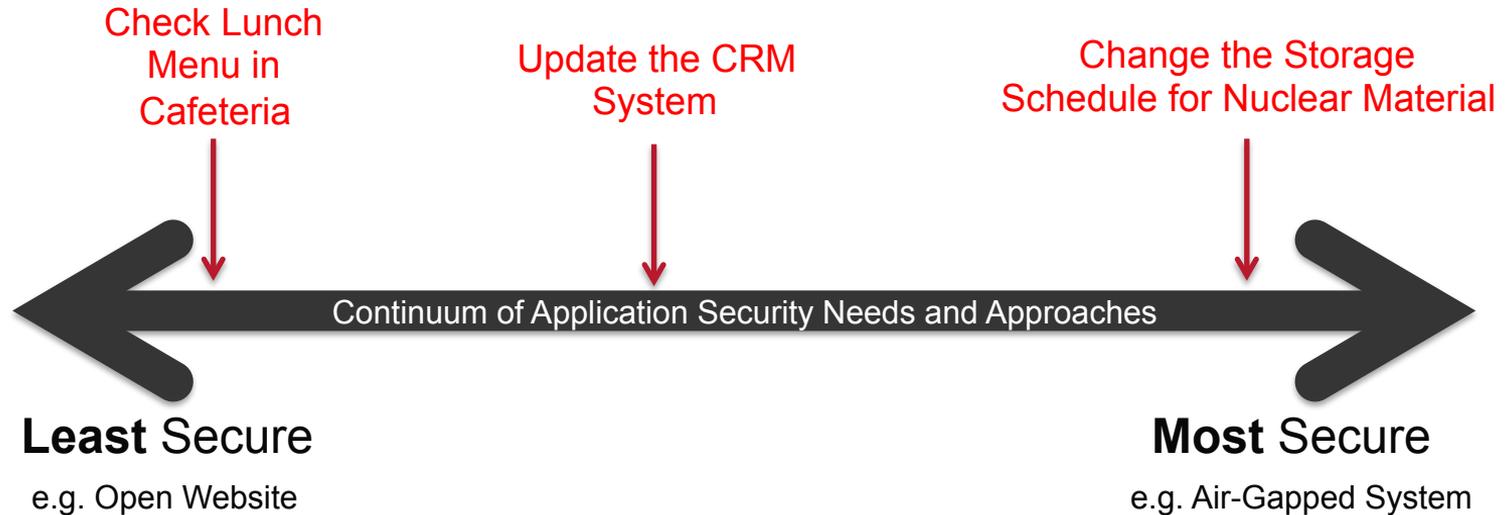
Least Secure

e.g. Open Website

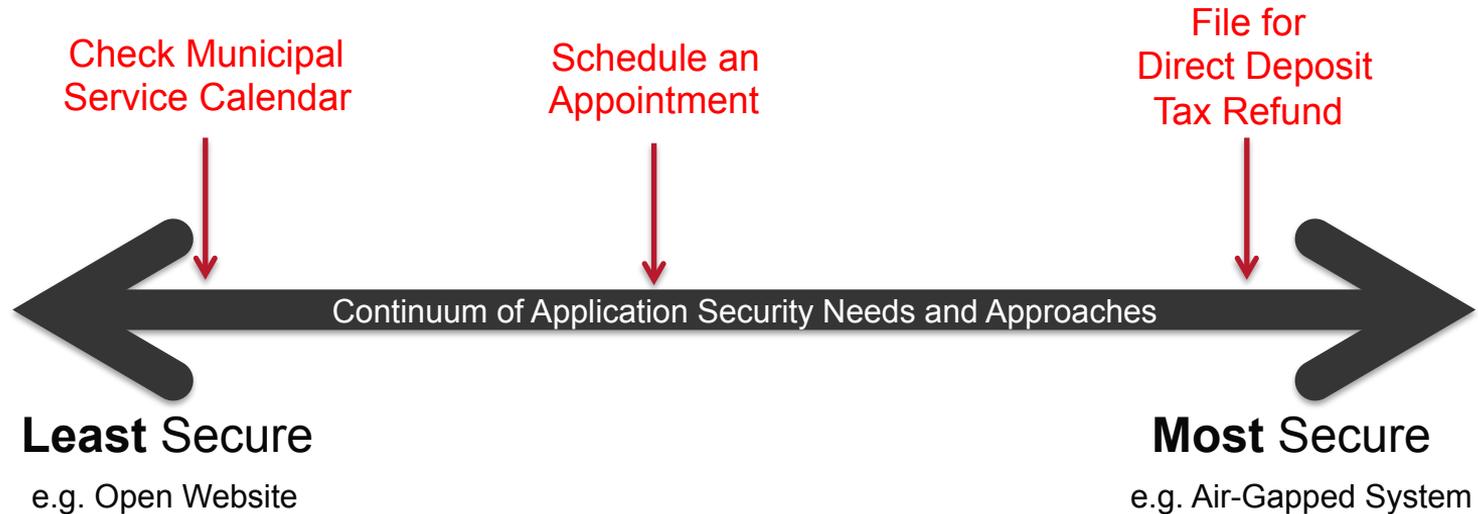
Most Secure

e.g. Air-Gapped System

Balancing Security and Convenience – B2E



Balancing Security and Convenience – B2C



Identity Assurance

Traditional Authentication is a ***one-time event*** and is too 'one size fits all'

- ▶ Made sense in homogeneous world – where all users have the same types of access and authentication devices.
- ▶ Doesn't work for modern heterogeneous world – where our end users have a variety of different access devices and authentication types/devices.
- ▶ Difficult to add new types of authentication
- ▶ Doesn't leverage a user's behavior as a factor in authentication.
- ▶ Not context aware.

Identity Assurance

Identity Assurance extends the concept of Authentication to:

- ▶ Enable the usage of a variety of different types of authentication available to different users for a given set of resources
- ▶ Leverage user behavioral information in determining the likelihood the user is who they claim to be. (location, time of day, resources being accessed, device type, new device).
- ▶ Leverage information about the context of the request to determine the type of authentication that is required. (on network, enterprise device vs. off-network rooted device)
- ▶ Enable administrators to define the level of assurance that is required for a given application, and the policies that determine how a certain level of assurance can be met.
- ▶ Enable OTHER administrators to define the level of sensitivity for a given application or resource.

The Problem: Islands of Identity



Applications traditionally designed to manage their own users!

Result 1: Poor UX, User Frustration,
Decreased Productivity, and
Decreased Interaction



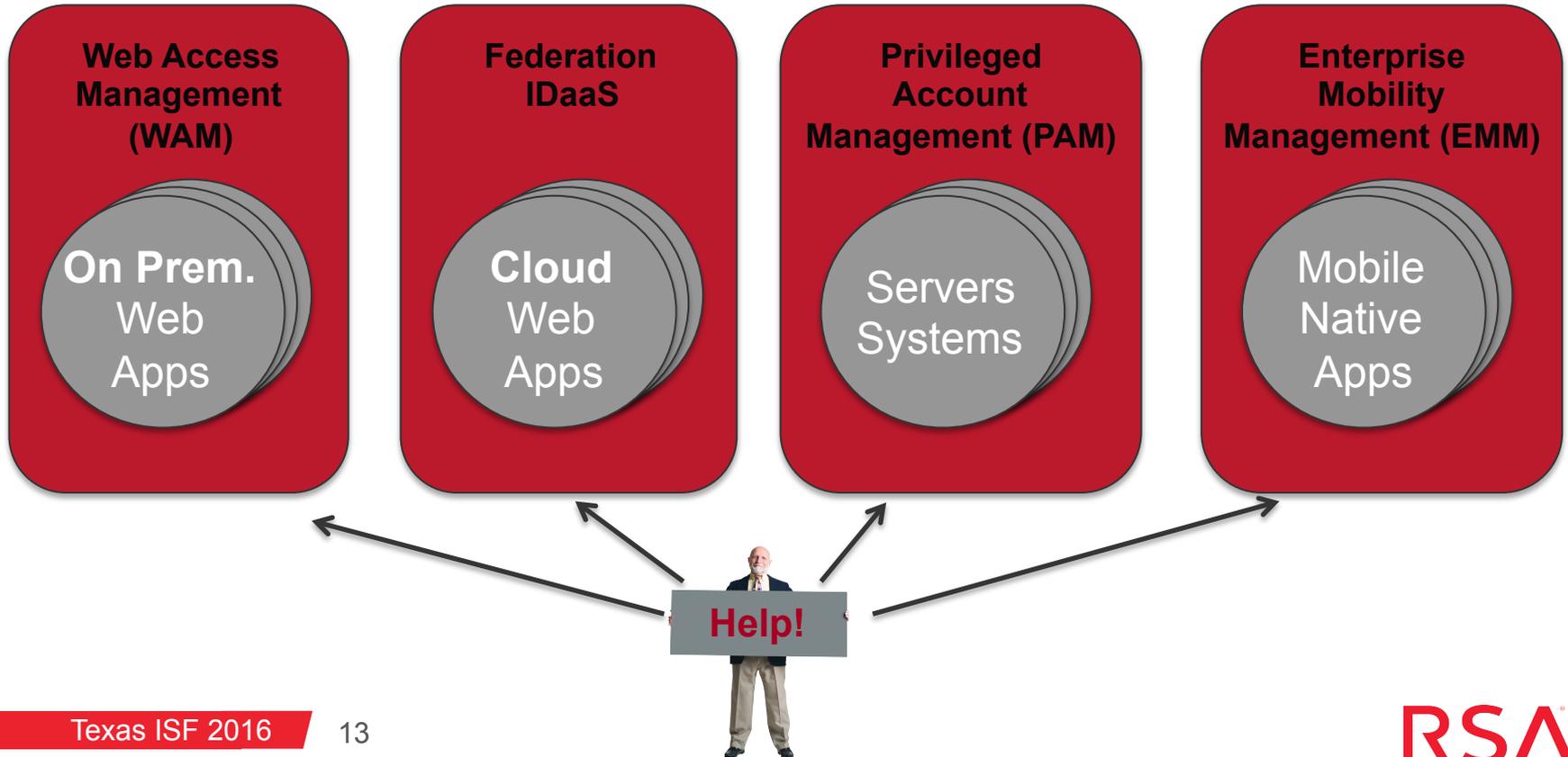
Result 2: Poor Security due to management of redundant data.
Common and/or Weak Passwords
Writing Down Passwords
Orphaned Accounts
Over-privileged Access
Poor Visibility for IT



We're Building Bridges

- ▶ Enterprises have implemented IAM technologies to mitigate (WAM, Federation, Directory). Builds secure 'bridges' between the islands – effectively creating bigger islands.
- ▶ SSO standards are now widely deployed – we must pressure our app vendors to do a better job at leveraging/embracing them. Great to see uptake in VPNs. Long tail will always exist though.
- ▶ We must build a standards-based identity platform to support all of the different types of applications that we provide/secure. Web, Cloud, VPN, Physical,

Where Are Those Islands and Bridges?



Recommendations

- ▶ Adopt a flexible approach to authentication that reduces the amount of ‘friction’ an end user feels to what is appropriate based on the sensitivity of the resource **and** the context of the request.
- ▶ Make your “Identity Islands” bigger. Leverage standards-based Identity systems and integration approaches wherever possible. Look for application vendors that support federated identity standards like SAML and/or OpenID Connect. This will make it so that as many applications as possible can leverage a common identity platform, providing the security and visibility that is required.
- ▶ Use Governance and Lifecycle solutions that will manage a user’s information through the entire span of their engagement with your enterprise. Ensure that the appropriate people can approve and attest to individual access rights. Ensure that your systems are actually enforcing the rules that you’ve defined.

Thank You

Darren Platt
darren.platt@rsa.com

