



**Where the \*\$&% is my identity?**

---

## Where the \*\$&% is my identity?



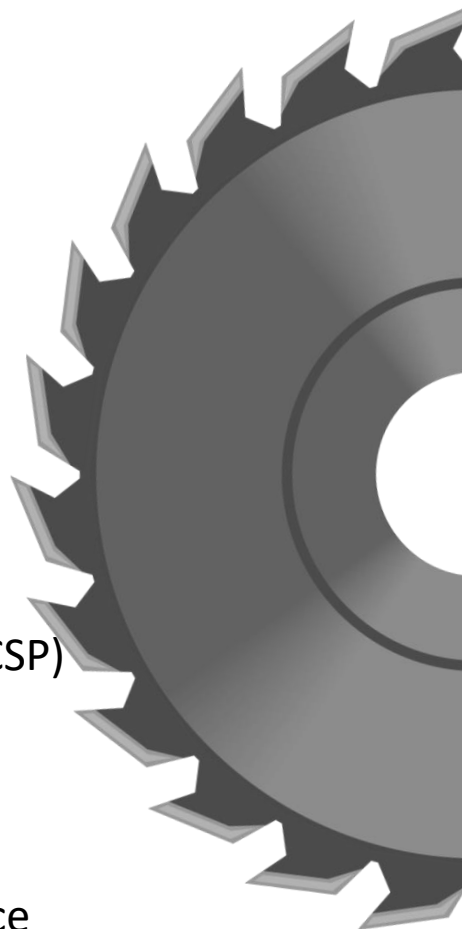
University of Colorado  
Denver | Anschutz Medical Campus

## Chris Edmundson – SANS Instructor

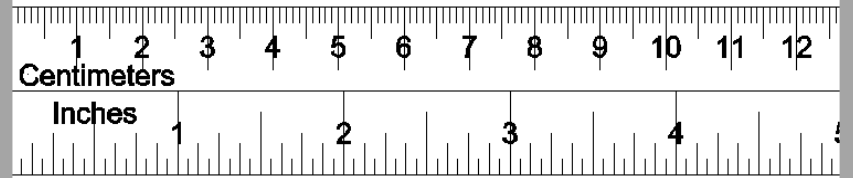
- GIAC Information Security Professional (GISP)
- GIAC Security Essentials (GSEC)
- GIAC Certified Forensic Analyst (GCFA)
- GIAC Security Leadership (GSLC)
- GIAC Certified Incident Handler (GCIH)
- GIAC Systems and Network Auditors (GSNA)
- GIAC Penetration Tester (GPEN)
- GIAC Mobile Device Security Analyst (GMOB)
- Global Industrial Cyber Security Professional (GICSP)
- GIAC Critical Controls Certification (GCCC)
- ITILv3 for IT Service Management
- TOGAF for Enterprise Architecture
- CCSK certification from the Cloud Security Alliance

<https://www.sans.org/course/auditing-networks-perimeters-systems>

<https://www.sans.org/profiles/chris-edmundson/>



# MEASURE TWICE



# CUT ONCE

Where the \*\$&% is my identity?

**Quick poll: What is the most common and expensive attack vector?**

- A) Malicious attacks
- B) System glitches and human error
- C) Insider attack
- D) SPAM

## Quick poll: What is the most common and expensive attack vector?



- “Malicious attacks were the most common and most expensive root cause of breaches”
- “Substantially longer to identify and contain a breach in the case of a malicious attack: a combined 314 days”
- “breaches caused by a malicious attack were 27 percent more costly than breaches caused by human error (\$4.45 million vs. \$3.5 million)”
- “Breaches from human error and system glitches were still the root cause for nearly half (49 percent) of the data breaches studied”
- “System glitches and human error breaches are still costly, with an average loss of \$3.24 million and \$3.5 million respectively”

Where the \*\$&% is my identity?

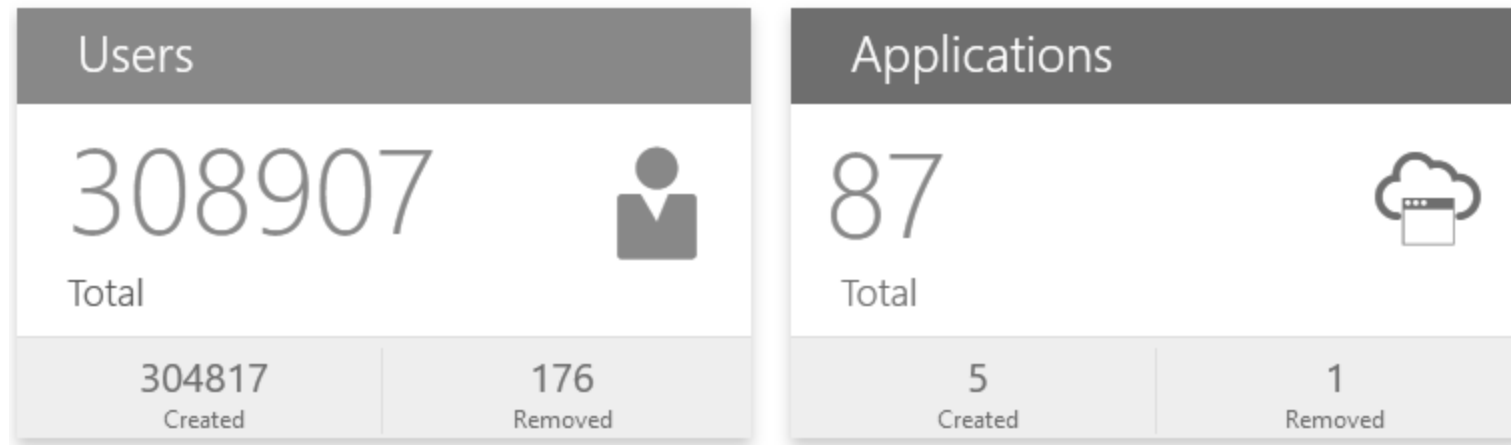
## What is identity and access management (IAM)?

- Identity and access management (IAM) in enterprise IT is about defining and managing the roles and access privileges of individual network users and the circumstances in which users are granted (or denied) those privileges. Those users might be customers (customer identity management) or employees (employee identity management). The core objective of IAM systems is one digital identity per individual. Once that digital identity has been established, it must be maintained, modified and monitored throughout each user's "access lifecycle."
- Identity management (IdM), also known as identity and access management (IAM or IdAM), is a framework of policies and technologies for ensuring that the proper people in an enterprise have the appropriate access to technology resources. IdM systems fall under the overarching umbrellas of IT security and data management. Identity and access management systems not only identify, authenticate, and authorize individuals who will be utilizing IT resources, but also the hardware and applications employees need to access.[1] Identity and access management solutions have become more prevalent and critical in recent years as regulatory compliance requirements have become increasingly more rigorous and complex.[2]

<https://www.csoonline.com/article/2120384/what-is-iam-identity-and-access-management-explained.html>  
[https://en.wikipedia.org/wiki/Identity\\_management](https://en.wikipedia.org/wiki/Identity_management)

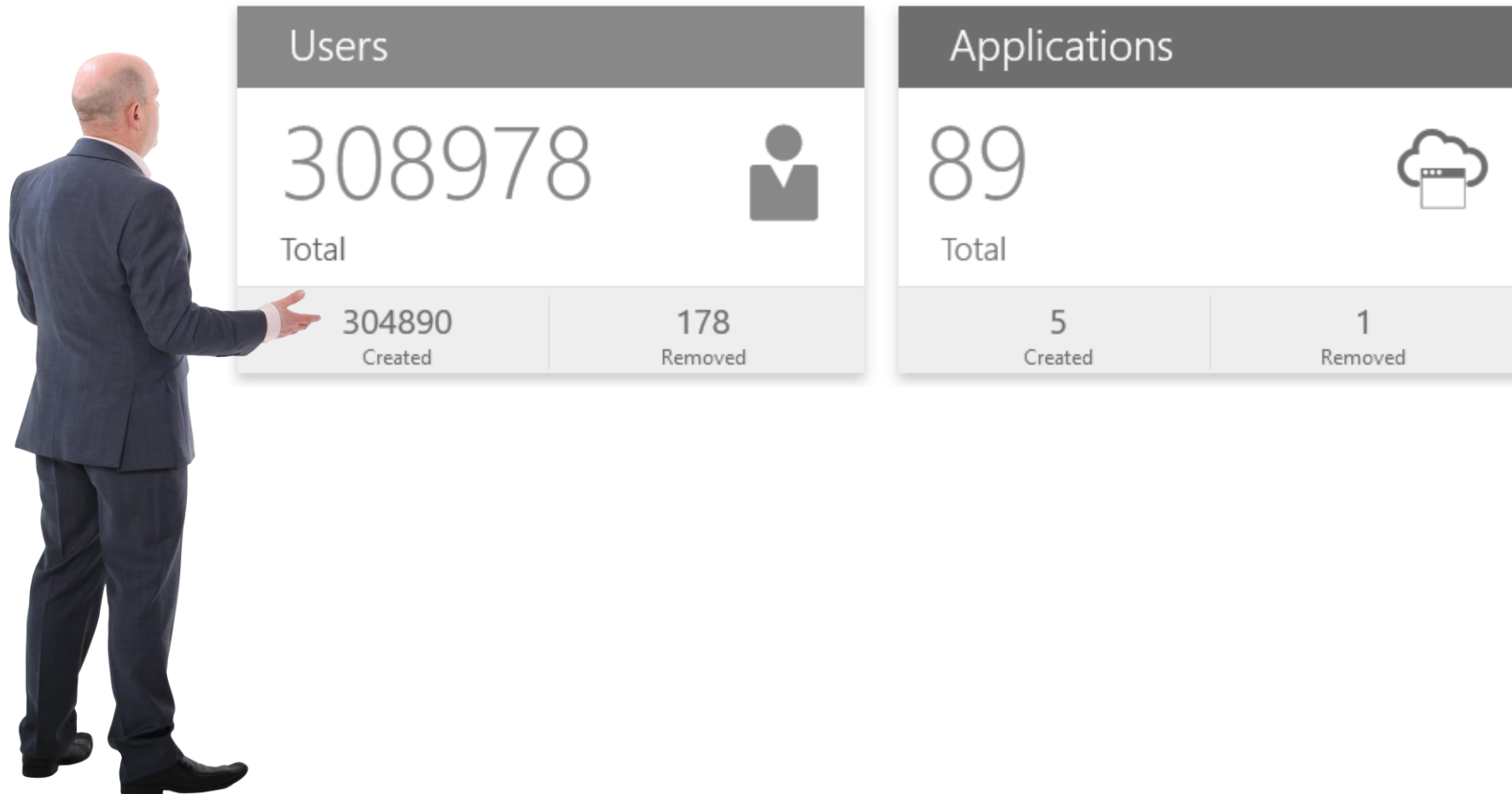
Where the \*\$&% is my identity?

**So you think IAM is static content? - a typical identity analytics dashboard**



Where the \*\$&% is my identity?

**Nope, IAM is very dynamic in nature**





## The Laws and Flaws of Identity; a few references

- 2005 - The Laws of Identity by Kim Cameron, Architect of Identity, Microsoft Corporation
  - “seven essential laws that explain the successes and failures of digital identity systems”
    - User Control and Consent
    - Minimal Disclosure for a Constrained Use
    - Justifiable Parties
    - Directed Identity
    - Pluralism of Operators and Technologies
    - Human Integration
    - Consistent Experience Across Contexts
- 2008 - The Seven Flaws of Identity Management: Usability and Security Challenges by IEEE

<https://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf>

<https://ieeexplore.ieee.org/document/4489846>



Where the \*\$&% is my identity?

**Quick Poll – what is the average cost per record lost in the U.S.?**

- A) \$100
- B) \$200
- C) \$150
- D) \$250

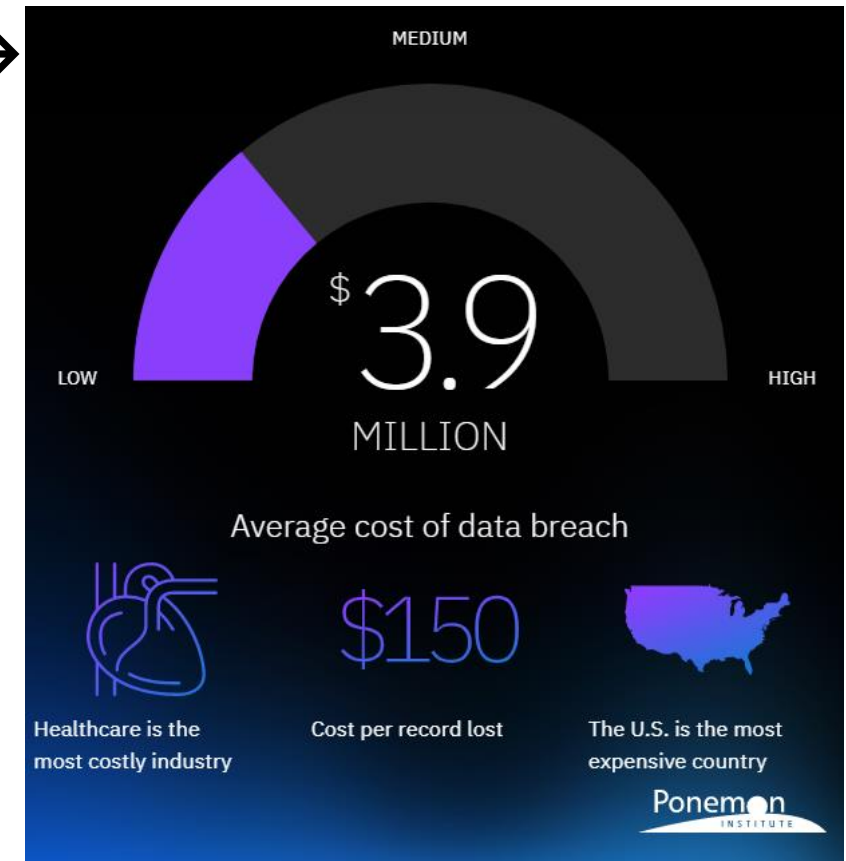
Where the \*\$&% is my identity?

## Quick Poll – what is the average cost per record lost in the U.S.

- According to the Ponemon Institute report →
- So, let's calculate the worst-case scenario:

300,000 identities \* \$150 = \$45,000,000

- Ouch!



## Where the \*\$&% is my identity?

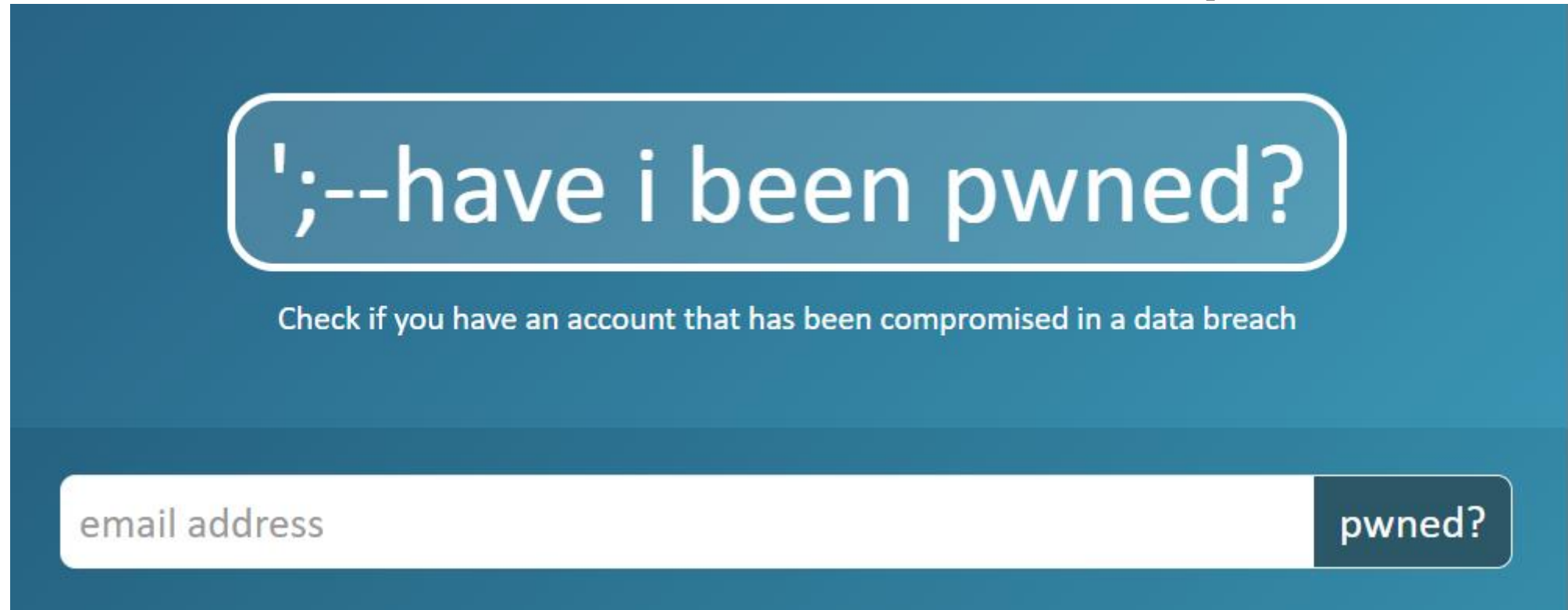
### So where is my identity? - a practical example – Zoom – Zoom – Zoom Reconnaissance and Discovery Activities / Potential Attack Vectors

- Directories / LDAP
- Application / Databases
- Data integration with 3rd party applications - API's, flat files
- Federated / Social Authentication
- IAM Provisioning
- Client Software / Agents
- Logs!! GET/POST data!!
- Our Challenge:
  - How do balance the user experience while securing their identity?

The screenshot shows the Zoom Cloud Meetings Sign In interface. It features a 'Sign In' heading, a form with 'Enter your email' and 'Enter your password' fields, a 'Forgot?' link, a 'Keep me signed in' checkbox, and a 'Sign In' button. To the right, separated by an 'or' divider, are three social login options: 'Sign In with SSO', 'Sign In with Google', and 'Sign In with Facebook'. A '< Back' link is at the bottom left, and a 'Sign Up Free' link is at the bottom right. Green arrows point from external labels to specific elements: 'Zoom?' points to the password field, 'IAM?' points to the 'Sign In with SSO' button, 'Google?' points to the 'Sign In with Google' button, and 'Facebook?' points to the 'Sign In with Facebook' button.

Where the \*\$&% is my identity?

## How do you know if your identity has been compromised?



The image shows a screenshot of the 'have i been pwned?' website. The main heading is 'have i been pwned?' in a large, white, sans-serif font, enclosed in a white rounded rectangle on a dark blue background. Below the heading, a smaller line of text reads 'Check if you have an account that has been compromised in a data breach'. At the bottom, there is a white input field with the placeholder text 'email address' and a dark blue button with the text 'pwned?'.

- IAM Analytics/Intelligence and IAM Governance!

Where the \*\$&% is my identity?

## IAM Governance

- Organizational Maturity Model
- High demand for People, Process, and Technical resources
- Tends to be complex and challenging for many organizations, so what do we do?



Where the \*\$&% is my identity?

**Given the hybrid nature of where identities are stored...**

- Let's fix the problem - sledge hammer approach?
- Purchase utilities for prevention, detection, remediation, etc. to protect IAM?
- Multi-Factor Authentication
- The promise of Cloud Access Security Brokers (CASB)
- API Management – including security policy, OAuth technologies, auditing and logging of traffic
- Governing IAM is difficult, so how can we further simplify?



Where the \*\$&% is my identity?

## Resource: Identity Management Testing - OWASP

- 4.3 Identity Management Testing
  - 4.3.1 Test Role Definitions
  - 4.3.2 Test User Registration Process
  - 4.3.3 Test Account Provisioning Process
  - 4.3.4 Testing for Account Enumeration and Guessable User Account
  - 4.3.5 Testing for Weak or Unenforced Username Policy

[https://owasp.org/www-project-web-security-testing-guide/latest/4-Web\\_Application\\_Security\\_Testing/03-Identity\\_Management\\_Testing/README](https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/03-Identity_Management_Testing/README)



## Resource: Leverage CIS Controls (version 7.1)

- # 4 - Controlled Use of Administrative Privileges
  - The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.
- # 12 - Boundary Defense
  - Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.
- # 16 - Account Monitoring and Control
  - Actively manage the life cycle of system and application accounts - their creation, use, dormancy, deletion - in order to minimize opportunities for attackers to leverage them.

Where the \*\$&% is my identity?

## **Resource: Cloud Security Alliance - Identity and Access Management**

- 2.3 Identity Management Services
  - 2.3.1 Provisioning and Deprovisioning
  - 2.3.2 Centralized Directory Services
  - 2.3.3 Privileged User Management
- 2.4 Authorization and Access Management
  - 2.4.1 Authorization Management
  - 2.4.2 Access Policy Management
  - 2.4.3 Audit and Reporting

[https://downloads.cloudsecurityalliance.org/initiatives/secaas/SecaaS\\_Cat\\_1\\_IAM\\_Implementation\\_Guidance.pdf](https://downloads.cloudsecurityalliance.org/initiatives/secaas/SecaaS_Cat_1_IAM_Implementation_Guidance.pdf)

Where the \*\$&% is my identity?

## Questions for Reflection & Guidance for Organizational Maturity

- Know thyself - are we leveraging the full potential of our IAM system?
- Does our strategic plan involve an on-premise only, completely cloud-based, or hybrid environment?
- If cloud-based environments are utilized, should we deploy CASB?
- Is our IAM solution meeting the needs for the dynamic information technology requirements with the technology transformations?
- Do our identity and access management processes fully secure 3<sup>rd</sup> party identities access to our environment? Are we auditing/monitoring the 3<sup>rd</sup> party access?
- Do we know all the privileged identities within our environment?
- What process do we have in place to detect, prevent, or remove unused or orphaned accounts?
- How do we leverage multi-factor to ensure the person's identity?
- Does our identity solution provide identity analytics showing how users access what they have been granted?
- Is our identity deployment providing the business value and outcomes we expect?



Where the \*\$&% is my identity?

## Chris Edmundson – SANS Instructor



- Questions
- Comments
- Conclusion

