ACUA
Association of College & University Auditors

March 24-26, 2026

ACUA VIRTUAL SPRING SUMMIT

Audit in Action

Identity And Access Management – Address The Root Causes

Johan Lidros

CISA, CISM, CDPSE, CGEIT, ITIL-F, CRISC, HITRUST CCSFP

March 25, 2026
10:30 PM – 12.20 PM

Presenter

Johan Lidros, Founder and President of Eminere Group

- Over 25 years of experience providing information technology security, compliance and governance services in Europe and in the United States, at many healthcare and higher education institutions.
- Well-versed in accepted IT and information security standards/frameworks (ISO27000, HITRUST, NIST, COBIT, CIS, TIR, etc.) and has participated in several related committees
- Certifications: CISA, CISM, CDPSE, CGEIT, ITIL-F, CRISC, HITRUST CCSFP
- ISACA certified instructor CISA, CISM, CRISC, CGEIT

Table of Contents

Introduction

Session Objectives:

1. Understand best practices in Identity and access management
2. How to best audit identity and access management to address the root causes
3. Key measurements and metrics to drive operational change
4. Be aware of tools and resources for identity and access management best practices.
5. Understand how AI impacts Identity and Access Management

The Solution – Sounds Simple

- Providing the right people with the right access at the right time.
- And then, over time, being able to prove it.
- Also, proving that access is changed as people's roles change and that you have removed access when they leave.
- IAM program with the right people, processes and Technology

IAM – Strategic Impact

- How critical is IAM for the organization's success?
  - Research
  - Student/Patient Safety
  - Operations
  - Financials
  - Intellectual Property
  - Student Communication/Satisfaction
  - Faculty alignment
  - Cyber risk
  - Recruiting
  - Cyber insurance
  - …

IAM

- Identity Management Services (IAM life cycle)
- Authentication Services (2FA, AD etc.)
- Access Management Services (role based, SSO)
- Privileged Account Management Services
- IAM Governance (SOD, regular reviews, monitoring, etc.)
- Log Management (certain part)
- IAM Program (Goals, gaps, roadmap, resources, cost, measurements, metrics)

The 2026 EDUCAUSE Top 10

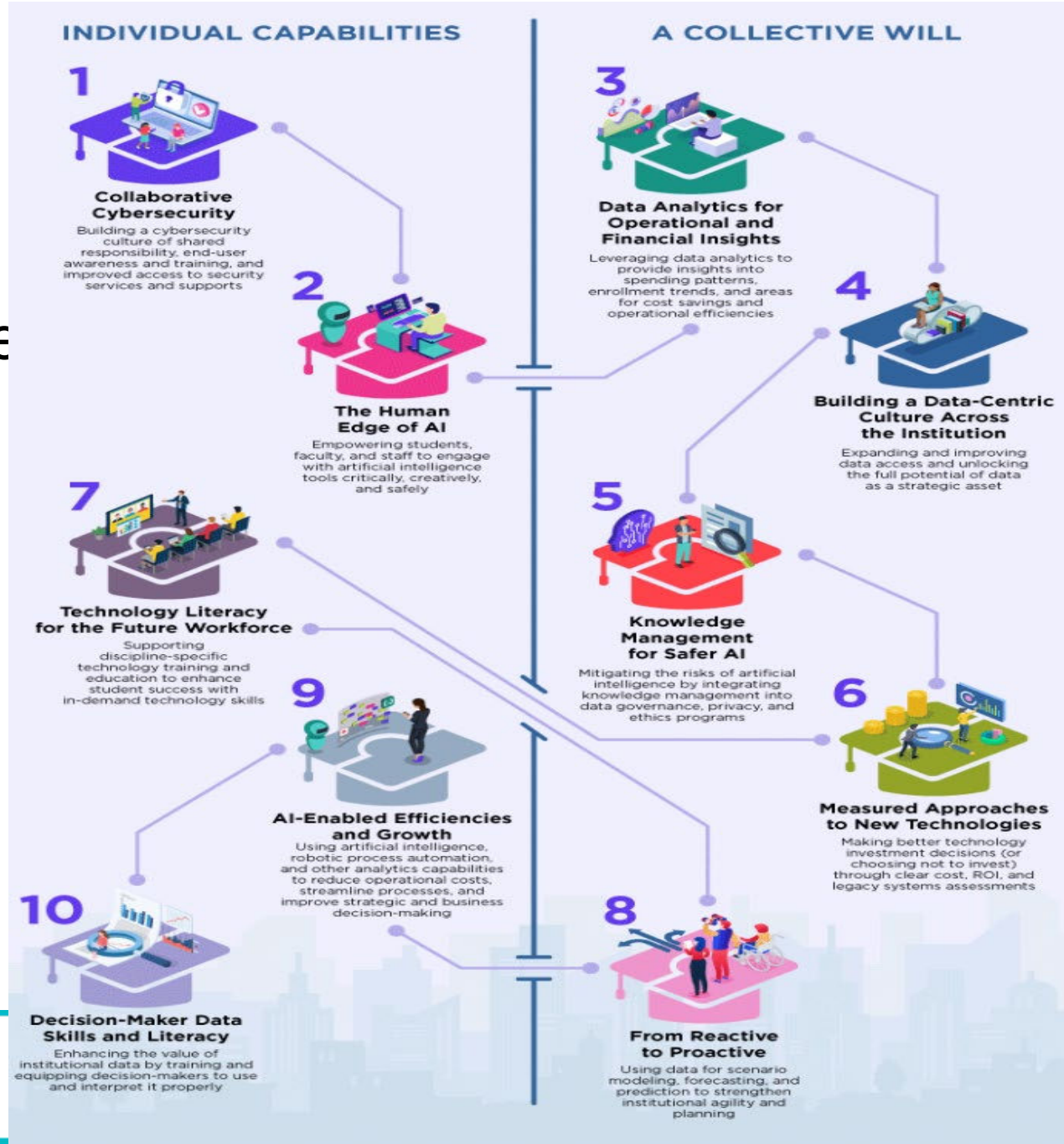
The 2026 EDUCAUSE Top 10 highlights how higher education technology and data leaders can foster a ***collective will*** and support ***individual capabilities***—two deeply connected actions that will help institutions thrive in the year ahead.

Educause 2026 Top Ten

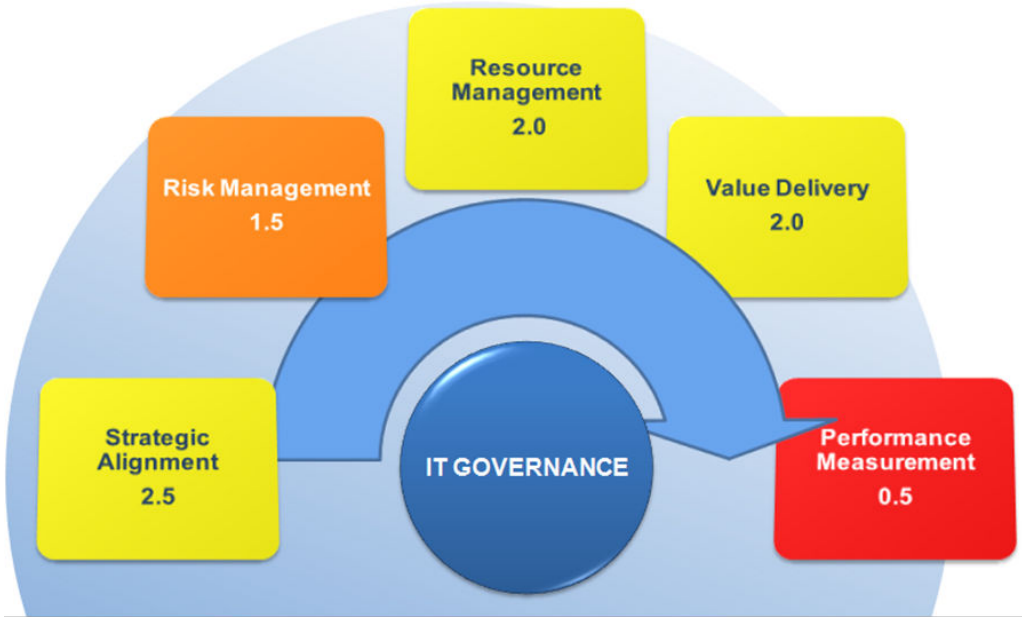
- **#1. *Collaborative Cybersecurity:*** Building a cybersecurity culture of shared responsibility, end-user awareness and training, and improved access to security services and supports
- **#2. *The Human Edge of AI:*** Empowering students, faculty, and staff to engage with artificial intelligence tools critically, creatively, and safely
- **#3. *Data Analytics for Operational and Financial Insights:*** Leveraging data analytics to provide insights into spending patterns, enrollment trends, and areas for cost savings and operational efficiencies
- **#4. *Building a Data-Centric Culture Across the Institution:*** Expanding and improving data access and unlocking the full potential of data as a strategic asset
- **#5. *Knowledge Management for Safer AI:*** Mitigating the risks of artificial intelligence by integrating knowledge management into data governance, privacy, and ethics programs
- **#6. *Measured Approaches to New Technologies:*** Making better technology investment decisions (or choosing not to invest) through clear cost, ROI, and legacy systems assessments
- **#7. *Technology Literacy for the Future Workforce:*** Supporting discipline-specific technology training and education to enhance student success with in-demand technology skills
- **#8. *From Reactive to Proactive:*** Using data for scenario modeling, forecasting, and prediction to strengthen institutional agility and planning
- **#9. *AI-Enabled Efficiencies and Growth:*** Using artificial intelligence, robotic process automation, and other analytics capabilities to reduce operational costs, streamline processes, and improve strategic and business decision-making
- **#10. *Decision-Maker Data Skills and Literacy:*** Enhancing the value of institutional data by training and equipping decision-makers to use and interpret it properly

2026 Top 10

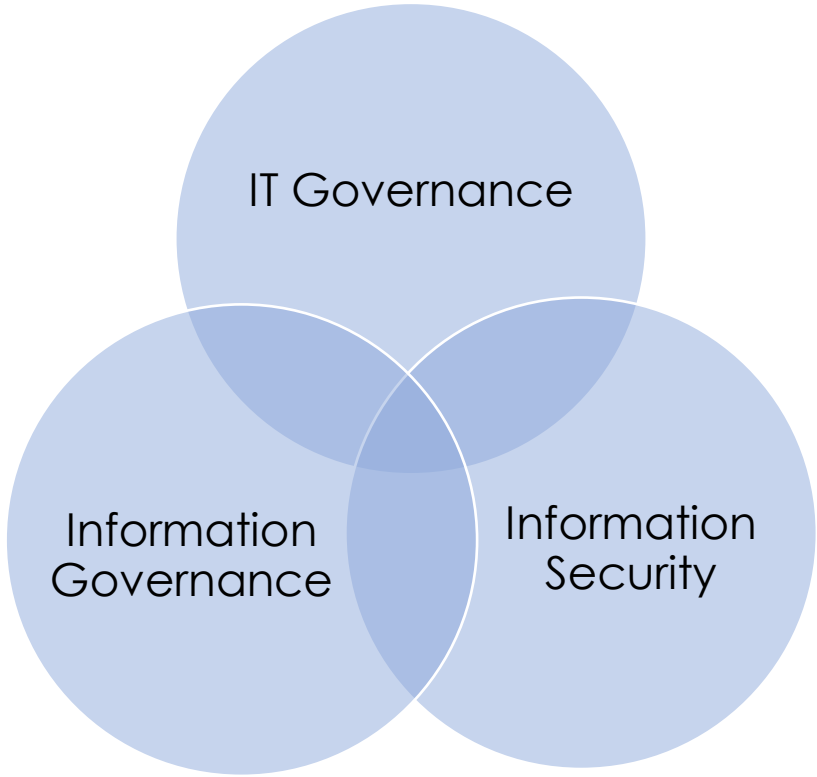
- The integration
- Change, change, change
- AI
- Data
- People….



The Foundational Aspects



Process Maturity Rating	
0	**Non-existent:** The process (control/procedures) does not exist.
1	**Initial/Ad hoc:** The process is informal, undocumented and reactive.
2	**Repeatable:** The process is repeatable but may be applied inconsistently as needed.
3	**Defined:** The process is documented and communicated.
4	**Managed:** The process is implemented and measurable.
5	**Optimizing:** Managed process with continuous performance improvements utilizing best practices.
N/A	**Not Applicable:** The process is not applicable to the review or has not been reviewed for other reasons.



Key IT Root Causes ….

- IT Governance
- Programs
  - Asset management
  - IAM/PAM
  - BCP/DRP/Resilience
  - Vulnerability Management
  - Incident Management
  - Information Security Program
- Risk Assessment integration
- IT Strategy
- Measurements/Metrics

Table of Contents

Typical Environment – Higher Education

- ~200 – 1000 “systems”
- How do we define systems?
  - OS and servers (unix, windows)
  - Databases
  - Applications
  - Mobile Apps
  - Network devices
  - Utilities and Tools – job scheduling systems, source code repository, virtualization (Vmware), firewalls, routers, sharepoint, others?
  - Medical Devices
  - Etc.
- What do you currently audit?
  - Application layer
  - Database layer
  - OS layer
  - Cloud layer (Entra)

Typical Audit – Identity & Access Management

- Enterprise risk analysis and risk based audit plan
  - What is the audit universe
- Perform risk analysis to determine scope of audit.
  - Do we really perform a risk analysis or do we just audit what we always audit?
- Perform the audit
- Identify control gaps/issues
- Generate recommendations (report, etc.)
  - What do we typically recommend?

Common IAM Audit Findings

- Not a comprehensive formally approved IAM program
- No clear business stakeholder/Information owner
- Inappropriate access/ Separation of duties
- Shared accounts
- Lack of approvals role matrices
- No regular reviews
- Excessive number of administrators/privileged users
- Service accounts (access to them, to privileged, not reviewed/documented)
- Alumni access….
- Role-based access not fully implemented
- “shadow IT”/decentralized IAM functions

Common IAM Audit Findings

- Terminated users still active
- The process to handle workforce changes…
- Password requirements
- Authentication requirements (2FA, Single Sign-on)
- Identification process
- Not a comprehensive repository of non-staff users (volunteers, researchers, contractors, etc.)
- Alumni accounts
- Password storage (service accounts)
- Weak policies
- Lack of formal procedures
- Lack of resources
- Lack of measurements
- Decentralized security – inefficient and ineffective

Common IAM Audit Findings

- Active Directory integration
  - Groups
  - Trusts
  - Cloud integration (Entra)
- Log management
- Others???

Table of Contents

Root Causes

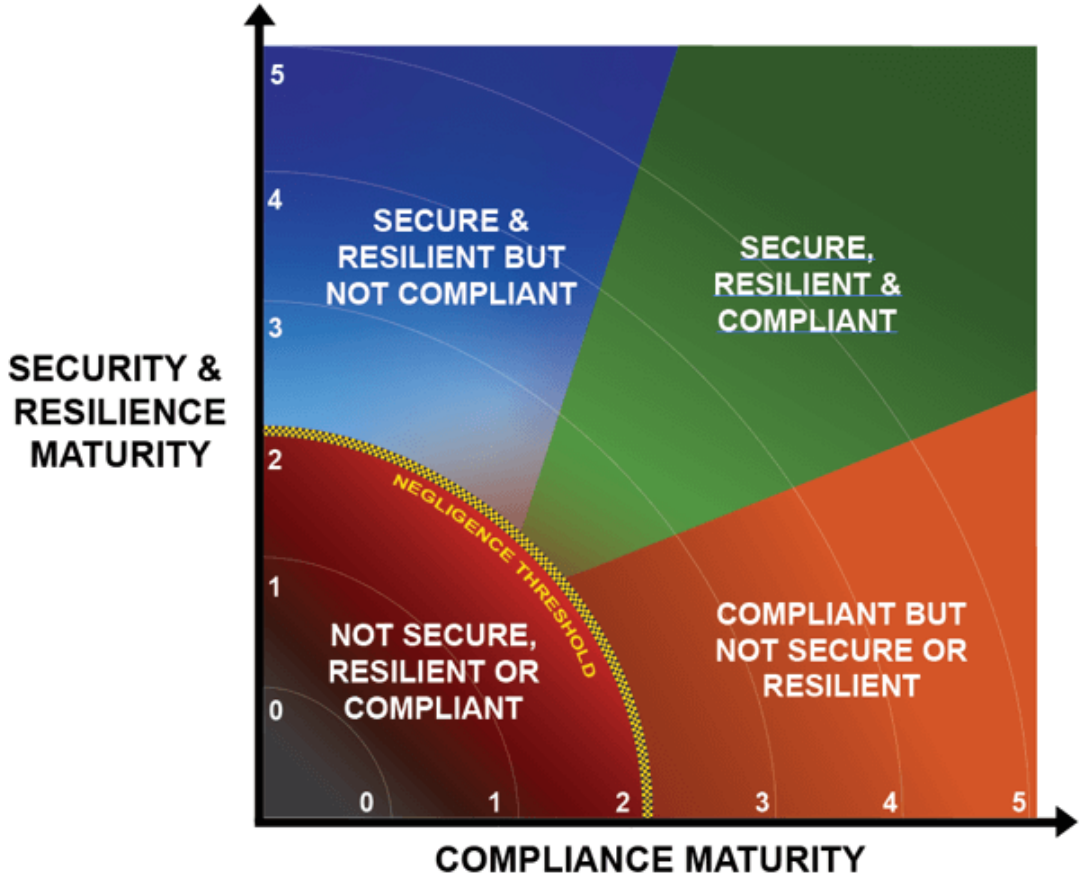
- Why do we continue to have the same issues re-occurring?
- Wrong audits?
- Wrong scope?
- Wrong recommendations?
  - Are we just recommending a temporary fix or addressing the root cause?
- What if we make the right recommendation?
    - IT or Management not addressing the issue – why?
      - Lack of funding
      - Resource intensive too fix
        - Not enough resources
        - Don’t have the right resources
      - Not a ‘priority’ – how do you balance fixing security issues vs addressing business or research related needs?

Root Causes

- Lack of information for decision-making
  - Wrong type of audit
  - Skillset audit team
  - Wrong observation
  - Wrong recommendations
- Roles and Responsibilities
  - Accountability (information owner/custodians)
  - Prioritization
  - Data governance
- Tool Support for IAM
  - Implementation
  - Wrong tool
- Resources/prioritization
- No or limited IAM program
- Limited measurements/metrics/reporting
- Culture (research, operation, education, faculty, etc.)
- Asset management program
- ….

What is Good Enough – Compliance or Resiliency?

- Compliance does not mean good risk management?
- What are the key risks?
- What is the status of key programs?
- Where does Quality come in?



Science and Information Security

Tool / Attribute	Availability	Integrity	Authenticity	Accepted Techniques	Authorization	Confidentiality	Credible Source	Reproducibility
3rd party data repo	O	O	O				O	O
Policy for network/cloud storage	N	O			N		N	
Archival storage	N	O					O	O
Workflow integrity checking		S						N
Access controls	N	N			S	N		
Physical security protections	N	N			N	N		
Network controls	N	N			N			
Logging	O	O			O			
Multifactor Authentication	O	O			O			
Intrusion detection/protection	O	O			O			
File/host integrity check	O	N			O			
RAID file system	N	N						
External backups	N	O						

Symbol	Meaning
S	Sufficient: This tool/technology alone can establish an assertion of the desired attribute, however weak it may be.
N	Necessary: This tool/technology is required to provide a stronger, credible assertion of the desired attribute.
O	Optional: This tool/technology can help strengthen the assertion of the desired attribute, however that is not its design intent.

Guidance for Trustworthy Data Management in Science Projects

https://trustedci.org/2020-trustworthy-data

September 30, 2020

Distribution: Public

Trustworthy Data Working Group

Andrew Adams, Kay Avila, Jim Basney, Laura Christopherson, Melissa Cragin, Jeannette Dopheide, Terry Fleury, Calvin Frye, Florence Hudson, Manisha Kanodia, Jenna Kim, W. John MacMullen, Mats Rynge, Scott Sakai, Sandra Thompson, Karan Vahi, John Zage

https://blog.trustedci.org/2020/10/tdwg-guidance-report.html

Cause of Cyber risks?

Consider a simple example: **A bank is robbed; that's the "what." The "how" might be that the burglar alarm failed to go off.** And that's usually the end of the story: There was an unfortunate malfunction.

But digging deeper, we might learn that the **alarm system was known to be old and unreliable. Funds had been allocated to replace it, but someone in management decided to instead use them for a marketing campaign to attract more customers.**

I call this **semiconscious decision-making**, because **someone made a decision** — not to replace the burglar alarm — **without considering the possible consequences of that choice, namely, losing all the cash**. In essence, that decision created the circumstance for the robbery.

The Rest of the Cybersecurity Story

Semiconscious decision-making is a common but too often unacknowledged cause of cyber risks.

Cause of Cyber risks?

Semiconscious decision-making is a common but too often unacknowledged cause of cyber risks.

The methodology is based on three core concepts:

(1) Identify the crown jewels — that is, what is it that you are trying to protect or prevent;

(2) (2) identify controllers for processes that are intended to protect the crown jewels; and

(3) (3) identify controllers for controllers, hierarchically.

In essence, an attack can only succeed if the needed controls were defective or simply not in place—and if a higher-level controller overlooked this security gap.

Applying the Cybersafety methodology in order to reveal the what, how, and why of the cyber event, we identified many cases of semiconscious decision-making that contributed to the Equifax data breach. These semiconscious decisions were made at all levels of the organization, from the middle management of technical groups to top executives and the board. Let's consider just some of those decisions.

- **Unencrypted data:** System out of scope. Management decided system out of scope for PCI audit i.e. not require encrypt data and be audited to ensure key controls in place.
- **Outdated certificates;** company's intrusion detection and prevention process (IDPP), which was supposed to be monitoring internet traffic for any messages that were suspicious or invalid, had not been functioning for at least nine months

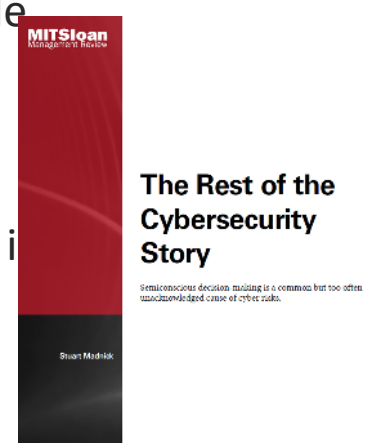
The Rest of the Cybersecurity Story

Semiconscious decision-making is a common but too often unacknowledged cause of cyber risks.

Cause of Cyber risks?

Why wasn't the IDPP functioning? It required certain security certificates to give it permission to access the internet traffic, but the certificates had expired — so it was not able to monitor any traffic or sound an alarm.

Why hadn't the certificates been updated long ago? Well, Equifax had hundreds, if not thousands, of such certificates, and tracking each one's expiration date and updating the certificates was an error-prone, manual task (not unlike the defective burglar alarm process i the bank robbery example).



The Rest of the Cybersecurity Story

Semiconscious decision-making is a common but too often unacknowledged cause of cyber risks.

This problem had been noted in the past; in fact, a proposal had been made to develop an automated, centralized certificate-management process. **But the managers responsible for the numerous applications requiring security certificates, scattered throughout the organization, did not consider this a priority. Furthermore, providing centralized support for managing the certificates would require some organizational changes that were likely to be resisted by those who had overlooked the danger created by expired certificates.**

Cause of Cyber risks?

Conscious Risk Assessment

Apparently, no one at Equifax considered the possibility that these two isolated decisions, along with many other similar semiconscious management decisions, might cost the company dearly. The **company's board essentially allowed management to take unmeasured, and thereby unlimited, risks** in order to pursue an aggressive growth strategy.

Although all of Equifax's board members had considerable experience in areas such as executive leadership and strategy development, **only two of the 10 had any expertise in cybersecurity**, according to company reports. (We found this to be a common element at the top of most of the organizations we studied.)

It is fine for management to have a "risk appetite," but when it comes to cybersecurity, the risk potential must be consciously and realistically evaluated. Most attacks that we studied stemmed from decisions made without any explicit consideration of risk. **The connections between decisions that might seem minor and the significant consequences those decisions can invite are rarely considered.**

While some risks are true surprises unlikely to be recognized in advance, many are more like the burglar alarm known to be defective. Indeed, in almost every case that we studied there were **red flags — often many of them — that management chose to ignore,** with disastrous consequences.

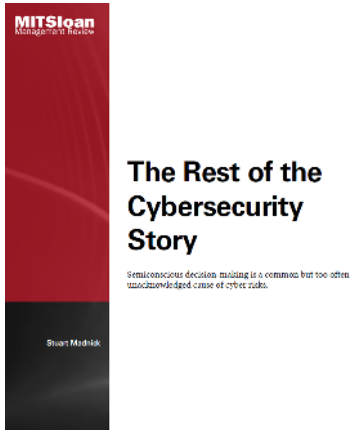
The Rest of the Cybersecurity Story

Semiconscious decision-making is a common but too often unacknowledged cause of cyber risks.

Cause of Cyber risks?

What to do

- **Management at every level must gain knowledge about how cyber risks arise and hone their skills in assessing the potential consequences of breaches**. Reading detailed analyses of past cyberattacks, such as those at Equifax and Capital One, and participating in tabletop exercises and cyber fire drills, are a couple of ways to accomplish this.
- When managers at all levels are developing plans to improve revenues or reduce costs, they **must consciously and deliberately assess the potential cyber risk of the planned changes — and then, only if the risk is acceptable, proceed.** Taking these steps can dramatically reduce the number of cyberattacks your company faces while minimizing the impact of any attacks that do successfully breach your systems.

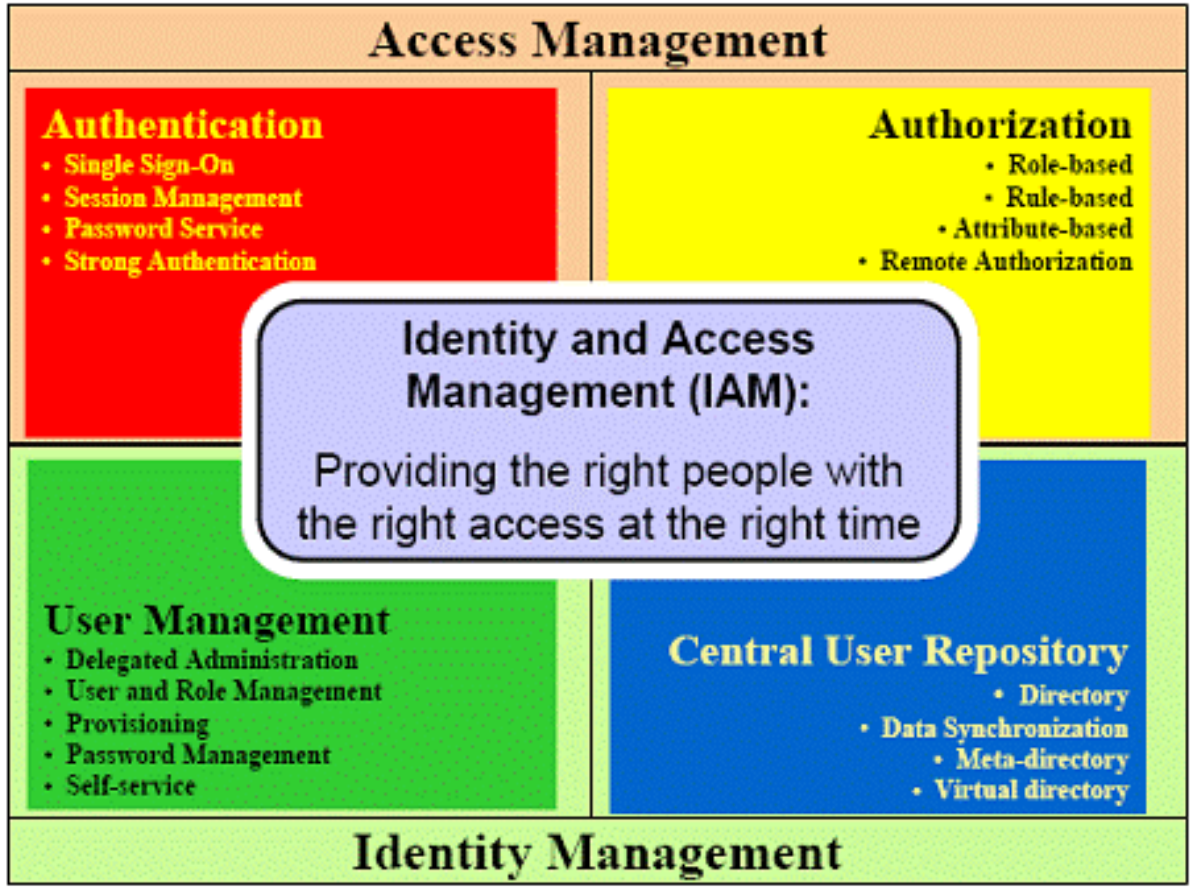


Learning points

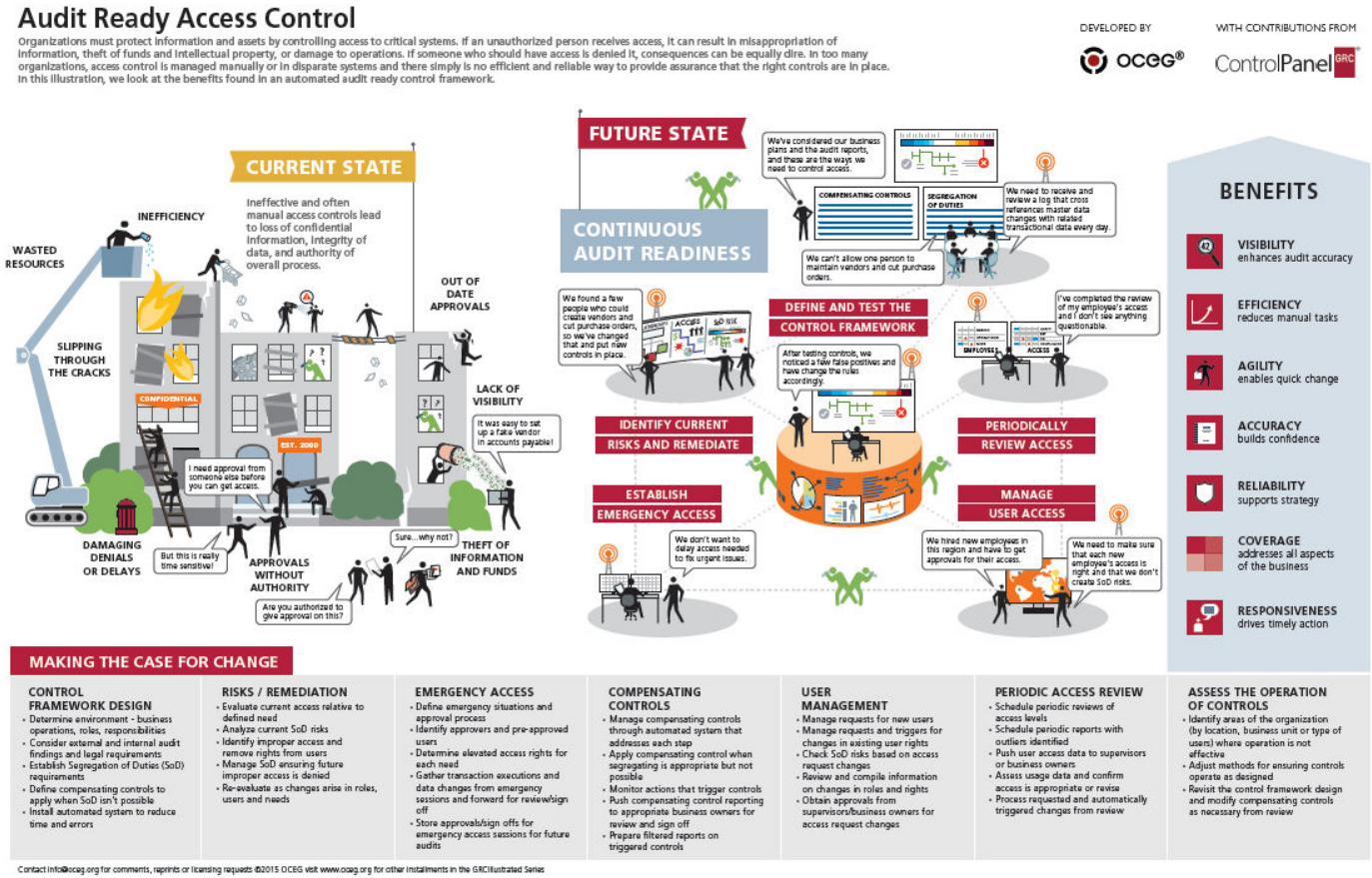
- Identify key Controls
- Risk versus cost
- Risk management process
- Who is involved make these “risk” decisions
- Politics
- Exception management
- Measurements and metrics

Table of Contents

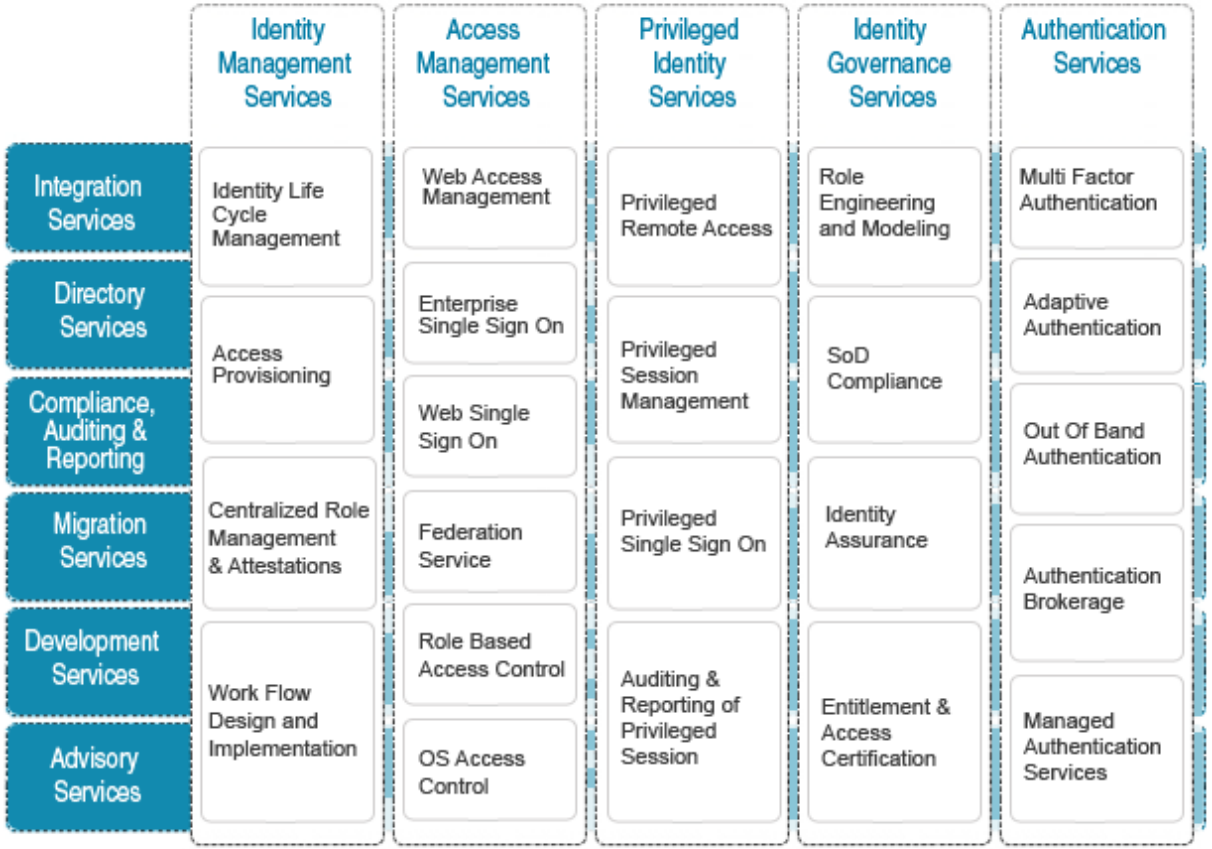
IAM


Access Management
Authentication
• Single Sign-On
• Session Management
• Password Service
• Strong Authentication
Authorization
• Role-based
• Rule-based
• Attribute-based
• Remote Authorization
Identity and Access Management (IAM):
Providing the right people with the right access at the right time
User Management
• Delegated Administration
• User and Role Management
• Provisioning
• Password Management
• Self-service
Central User Repository
• Directory
• Data Synchronization
• Meta-directory
• Virtual directory
Identity Management

Processes – OCEG framework



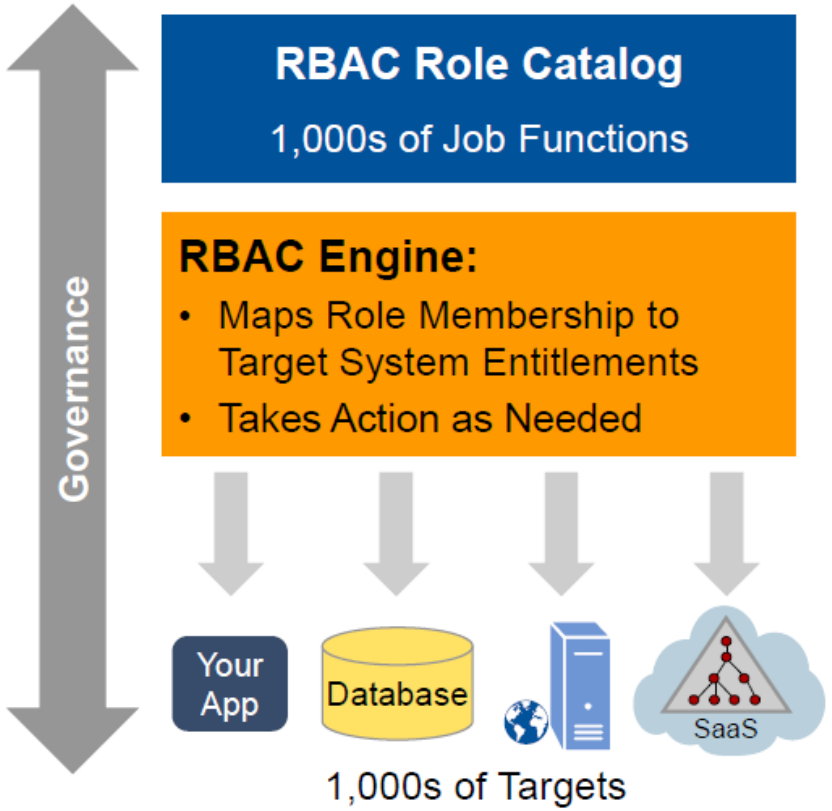
IAM


Identity Management Services
Access Management Services
Privileged Identity Services
Identity Governance Services
Authentication Services
Integration Services
Directory Services
Compliance, Auditing & Reporting
Migration Services
Development Services
Advisory Services
Identity Life Cycle Management
Access Provisioning
Centralized Role Management & Attestations
Work Flow Design and Implementation
Web Access Management
Enterprise Single Sign On
Web Single Sign On
Federation Service
Role Based Access Control
OS Access Control
Privileged Remote Access
Privileged Session Management
Privileged Single Sign On
Auditing & Reporting of Privileged Session
Role Engineering and Modeling
SoD Compliance
Identity Assurance
Entitlement & Access Certification
Multi Factor Authentication
Adaptive Authentication
Out Of Band Authentication
Authentication Brokerage
Managed Authentication Services

IAM

- Identity Management Services (IAM life cycle)
- Authentication Services (2FA, AD etc.)
- Access Management Services (role based, SSO)
- Privileged Account Management Services
- IAM Governance (SOD, regular reviews, monitoring, etc.)

IAM - Implementation



Business Ownership

Access Governance:

- Role Description
- Role Membership
- Segregation of Duties
- Approval Process

IT Ownership

Technology Implementation:

- Role Entitlements per Target
- Plumbing the Connector

What is Computable Privacy? Example

- To achieve health, an individual's electronic health data need to be digitally connected to their consent choices.
- Health care providers, and their health IT systems need to know what to do when the individual does not document a choice.
- Telemedicine, community health supports, and other innovative delivery processes will be stunted if we cannot make privacy computable.

This is HIPAA

Why IAM Fails

Reason #5: Failure to plan/govern/fund/prioritize.
Reason #4: Failure to engage the proper stakeholders.
Reason #3: Automating the existing flawed processes.
Reason #2: Trying to “Boil the Ocean” with a “Big Bang” approach.

And, the #1 Reason IAM projects fail:

Treating IAM as a Stand-alone IT Tool

Success Factors

- ✓ Focus more on process than technology.
- ✓ Implement a sound IAM program that embraces common governance, architecture, and project management.
- ✓ Treat core project team like your family:
  - Long-term continuity, retention incentives.
  - Avoid people churn — causes fits and starts.
  - Insulate team from mindless business distractions.
- ✓ Invest in a strong IAM champion/evangelist:

Sample Key Measurements

- Number of resources – performing access management related tasks
- Number of audit findings
- Volume
  - Systems
  - Requests
- Build Accountability
  - Data owners
  - Program owner (program)
- Business Aligned
  - Research
  - Education
  - Finance
  - School
  - Foundational systems

		Trend	Goal
Type and Number of Systems			
PHI	242	↓	150
PII	312	↑	250
Critical	85	↓	75
Number of FTE IAM	4	←	6
Number of Access Reviews	52 (15%)	↑	80%
Number of Access requests		↑	
-Initial	2300	↑	
-change	500	←	
-Terminations	500	↓	

Sample Key Measurements (cont.)

	Trend	Risk Level
Terminated Users		
Centralized Systems	↑	M
Decentralized Systems	↓	H
Cloud	↑	H
Appropriate Access	←	

Table of Contents

Proposed Audit Approach

- Full scale audit of Identity Access Management
  - Not just controls based audit – effectiveness and efficiency/value
  - Need to include decentralized, cloud based solutions in addition to centralized solutions
  - Assess resources
  - Assess tools
  - Assess processes
  - Assess training (IAM team, data owners, stewards, custodians)
  - Measurements
  - Total cost of ownership
  - Recommendations
    - Need to address root cause
    - Need to be prioritized
    - Need to be risk based
    - Need to assign business stakeholder(s as appropriate
  - Need to perform follow up / status reviews of prior audit findings

AI Impact

- Understand the AI technology
- “Service accounts” – access and authentication
  - Shift from static, human-centric reviews to dynamic, "Know Your Agent" (KYA) AI agents, chatbots, and machine learning models are now acting as autonomous identities that require oversight and lifecycle management.
- Data access
- Log management
- Change management
- IAM Tool impact

IAM - Goals

- Scalable and sustainable system
- Streamlined management of user identities and access rights
- Automate and reduce the time for assessments and reports
- Establish strong privacy and security policies not only within the enterprise but also throughout participation.
- Reduce overall cost of compliance (i.e., audits, penalties, remediation, etc.)
- Implement effective measurements to align with data owner and other stakeholders need.

Solution Drivers

- Business - lowering the cost of managing employees' permissions and minimizing the amount of time that users are without their necessary permissions;
- Security - ensuring information security, integrity, and availability;
- Research – Grant requirements (CMMC, NIH, private companies, etc.)
- Student/Patient Safety – Improve risk management
- Strategic – ensure business alignment improve key strategic needs/initiatives (faculty, business partner initiatives, student satisfaction, etc.)
- Regulatory – compliance with the Health Insurance Portability and Accountability Act (HIPAA), FERPA, and the Payment Card Industry Data Security Standards (PCI DSS)

Table of Contents

Resources

- Cobit 5 – comprehensive for information security principles, policy and framework
  - APO 13 Manage Security and other areas
  - *Identity and Access Management Audit Program*
  - Biometrics Audit Program
  - Cybersecurity Audit Program 2.0
  - AI Audit Toolkit
  - Zero Trust Audit program
  - Data base Audit program
  - Shadow IT Audit program
- ISO 27000 Serie Information Security Management System (ISMS) – an overarching management framework
  - ISO/IEC 24760-1 A framework for identity management—Part 1: Terminology and concepts
  - ISO/IEC CD 24760-2 A Framework for Identity Management—Part 2: Reference architecture and requirements
  - ISO/IEC WD 24760-3 A Framework for Identity Management—Part 3: Practice
  - ISO/IEC 29115 Entity Authentication Assurance
  - ISO/IEC WD 29146 A framework for access management
  - ISO/IEC WD 29003 Identity Proofing and Verification
  - ISO/IEC 29100 Privacy framework
  - ISO/IEC 29101 Privacy Architecture

Resources (continued)

- IIA
  - GTAG Workprogram Auditing Identity and Access Management
- NIST
  - Standards – SP 800 – 37, 53a, 60, 70 Special Publication
  - 800-63-3: Digital Authentication Guideline
  - Identity systems management program - http://www.nist.gov/itl/idms/index.cfm
  - Computer Security Resource Center - http://csrc.nist.gov/projects/iden_ac.html
  - NIST SPECIAL PUBLICATION 1800-9 – Access Rights Management for Financial Services
  - The attribute-based access control (ABAC) model https://csrc.nist.gov/News/2018/NIST-Researchers-Publish-Book-on-ABAC
  - NIST SP 800-207, Zero Trust Architecture
-

Resources (continued)

- The white papers…
  - CapGemini – Identity and Access Management
  - Gartner – various whitepapers and webinars
  - Sailpoint – various whitepapter
  - Webinars

- Health IT – ONC
  - SAFER Guides - https://www.healthit.gov/safer/
  - How to Identify and Address Unsafe Conditions Associated with Health IT

- Cloud Security Alliance – 12 domains identity and access management

- OCEG (Open Compliance and Ethics Group) – Audit Access Control https://go.oceg.org/illustration-audit-ready-access-control

Table of Contents

Conclusion

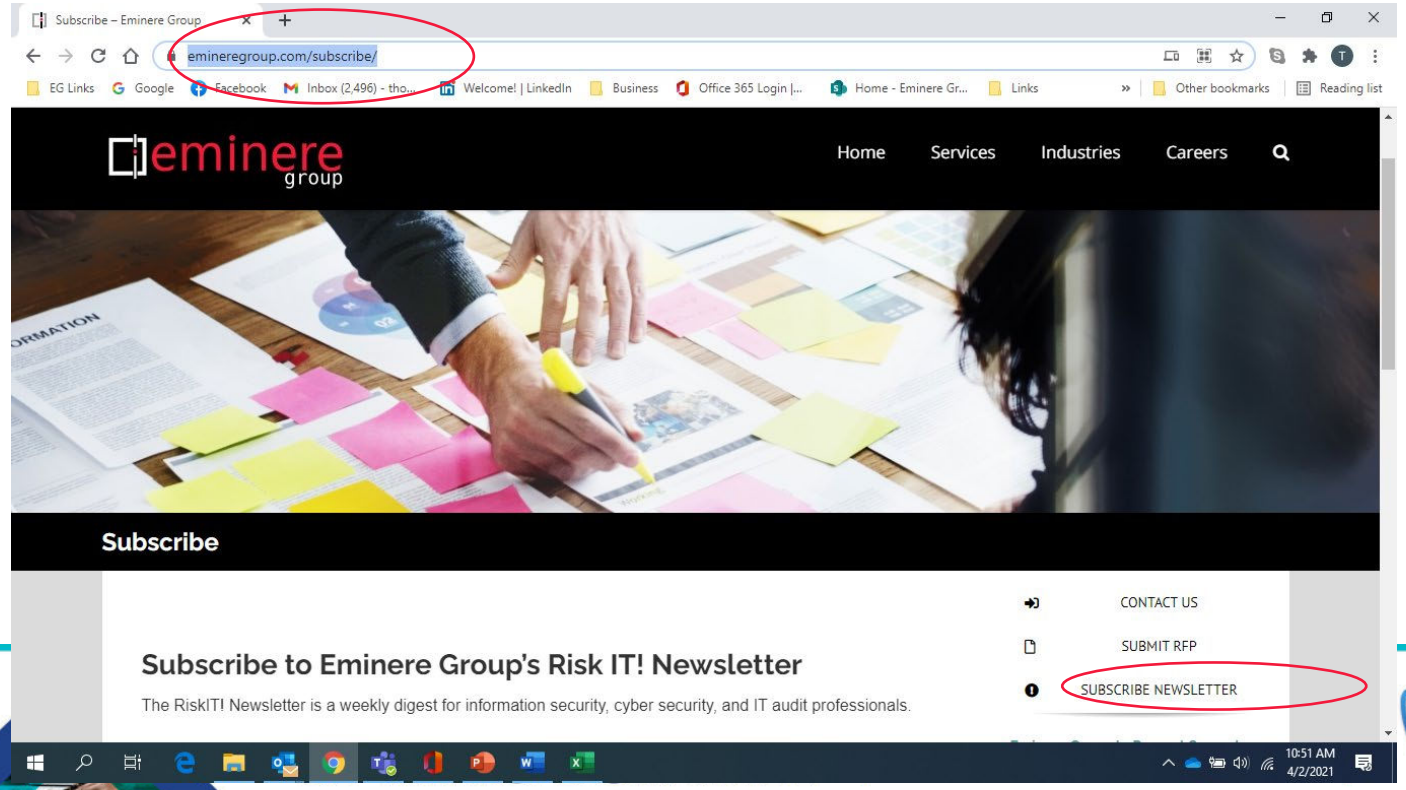
- Need to audit the program and practices
- Need to have the right audit scope
- Need to review key systems and supporting infrastructure
- Recommendations need to address root cause
- It is not an IT problem – Key success for safety, cyber security and strategic initiatives.

Table of Contents

Q & A

Ongoing IT Risk/Cybersecurity Updates

Interested in on-going IT Governance and IT Security updates? Sign up for our weekly newsletter “RiskIT “at https://www.emineregroup.com/subscribe/ or Linkedin Eminere Group Risk IT Newsletter



Johan Lidros Contact Information

Johan Lidros, President

johan.lidros@emineregroup.com
(813) 832-6672 x-9101
(813) 355-6104 (cell)

Connect on LinkedIn
linkedin.com/in/johanlidros
Or QR-code

Polling Question #1

What is your most critical System?

A. ERP (Banner, Peoplesoft, Workday)
B. Data Warehouse
C. Backup utility
D. Password/Encryption key vault
E. Active Directory
F. Online Banking
G. System manages “Asset” Inventory(ies) (data, software, hardware, interfaces, etc.)

Polling Question #2

Do you know the number of systems (cloud, onsite, etc.) in your organization?

A. 50-100
B. 101-200
C. 201-300
D. 301-400
E. 400-500
F. >500
G. Do not know

Polling Question #3

What percentage of your systems have a correct access review performed on a regular basis (annually)? This includes review and approved role matrices for all layers (OS/database/application) and all accounts (user, service, generic, privileged, etc.).

A. 100%
B. 75-99%
C. 50-74%
D. 25-49%
E. 1-25%
F. None
G. Do not know how many reviews

Question 4:

What systems require multifactor authentication (MFA)? Select all that apply.

A. All remote access
B. Most remote access
C. No remote access
D. Access to all onsite systems
E. Access to certain onsite systems
F. No MFA for onsite systems
G. Access to all cloud systems
H. Access to certain cloud systems
I. All systems containing PII
J. All privileged access
K. Only remote privileged access
L. No MFA
M. Do not know