Managing Technology Risk and Compliance for Business Success

Compliance and security frameworks can help your business identify, mitigate, and monitor technology risks

Qualifying for CPE

Remain in session for **50 minutes**

Respond to 4 **polling questions**

Complete post-session **survey**

Receiving CPE Credit

- Credit processed within 90 days after session
  - UHY Colleagues: Credit and certificate available in LCvista
  - External Colleagues: Credit w/ certificate sent from “UHY CPE”
- Credit questions should be directed to CPE@uhy-us.com
- Recordings/materials available 24 hours after session
  - UHY Colleagues: UHY University
  - External Colleagues: UHY’s event page

Introductions & Learning Objectives

About UHY

UHY is one of the nation’s largest professional services firms providing audit, tax, consulting and advisory services to clients primarily in the dynamic middle market.

We are trailblazers who bring our experience from working within numerous industries to our clients so that we can provide them a 360-degree view of their businesses. Together with our clients, UHY works collaboratively to develop flexible, innovative solutions that meet our clients’ business challenges.

As an independent member of UHY International, we are proud to be a part of a top 20 international network of independent accounting and consulting firms.

About the Presenter

David Barton

Managing Director

Technology, Risk & Compliance

Background

- Over 30 years of practical experience in information systems and technology risks and controls including extensive experience utilizing cybersecurity and compliance frameworks to minimize technology risk

Professional Experience

- System and Organization Controls (SOC) attestations including SOC 1, SOC 2, SOC 3, SOC for Cybersecurity
- Provides Technical Review for Wolters Kluwer CCH Audit tools for SOC
- Frequent speaker at national and regional security events, such as SecureWorld and the Cloud Security Alliance Congress. He is the primary author of the CSA position paper on AICPA Service Organization Control Reports
- **Education & Certifications**
- Masters in Business Administration, Appalachian State University
- B.S. in Business Administration, Appalachian State University
- Certified Information Systems Auditor (CISA)
- Certified in Risk and Information Systems Control (CRISC)

Objectives of Today's Session

Explore Common Business Risks in the Digital Age

Identify Effective Risk Management Techniques

Understand Common Compliance Frameworks

Strategies for Success

Common Business Technology Risks

- ## Data Breaches

  Unauthorized access to sensitive customer or proprietary data, leading to financial and reputation reputation damage.

- ## Cyber Attacks

  Malicious activities such as ransomware, phishing, phishing, business email compromise, and distributed distributed denial-of-service (DDoS) attacks, disrupting disrupting business operations and causing financial financial losses.

- ## Operational Disruptions

  Technology failures, system outages, and supply chain chain disruptions, leading to service interruptions and interruptions and reduced productivity.

- ## Third Party Risks

  Leveraging third parties to assist with common business business and IT functions has become common. Understanding the controls and processes at your third-your third-party providers is critical to risk management.

- ## Cloud and SaaS Risks

  Data privacy and security concerns, vendor lock-in, and in, and availability issues with cloud-based services and services and software-as-a-service (SaaS) applications. applications.

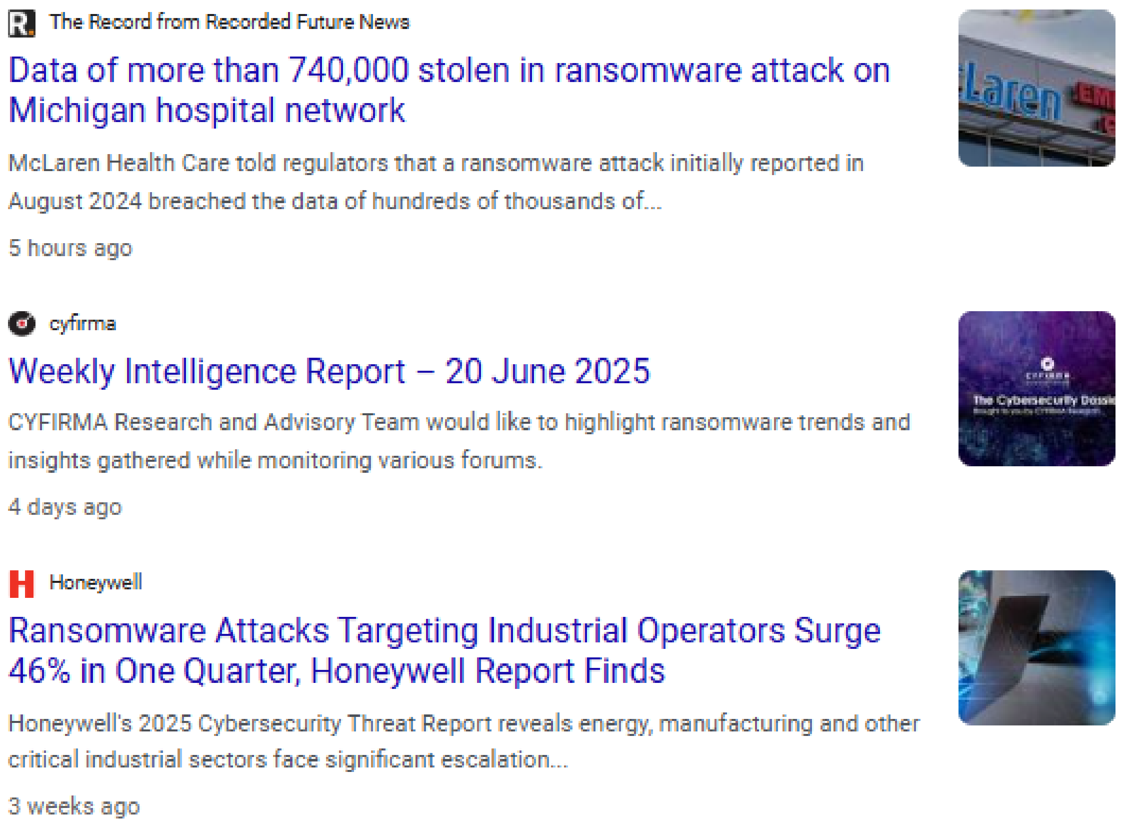
- ## Industry Non-compliance

  Failure to adhere to regulations and data protection protection laws, resulting in fines, legal liabilities, and and brand damage.

Recent Breaches

- In February ***Grubhub*** announced a data breach that affected both its customers and drivers. Hackers were able to gain access to a variety of personal data, including names, email addresses, and phone numbers. The intrusion happened through a third-party service used by Grubhub's customer support team.
- ***Hertz*** rental car had data stolen as the result of a vulnerability found in Cleo, a third-party file-sharing service used by the company. Hackers were able to steal not only names, contacts, birth dates, credit cards, and driver's license information, but also sensitive data from car accident claims, including social security numbers, government IDs, and medical details.
- Cybersecurity firm ***Picus Security*** shared a new report earlier this year that found that cyberattacks on password managers have tripled compared to 2024. The company's researchers discovered that out of more than a million types of malware, 25 percent of them were specifically targeting password managers.

Recent Cyber Attacks



The Record from Recorded Future News

Data of more than 740,000 stolen in ransomware attack on Michigan hospital network

McLaren Health Care told regulators that a ransomware attack initially reported in August 2024 breached the data of hundreds of thousands of...

5 hours ago

cyfirma

Weekly Intelligence Report – 20 June 2025

CYFIRMA Research and Advisory Team would like to highlight ransomware trends and insights gathered while monitoring various forums.

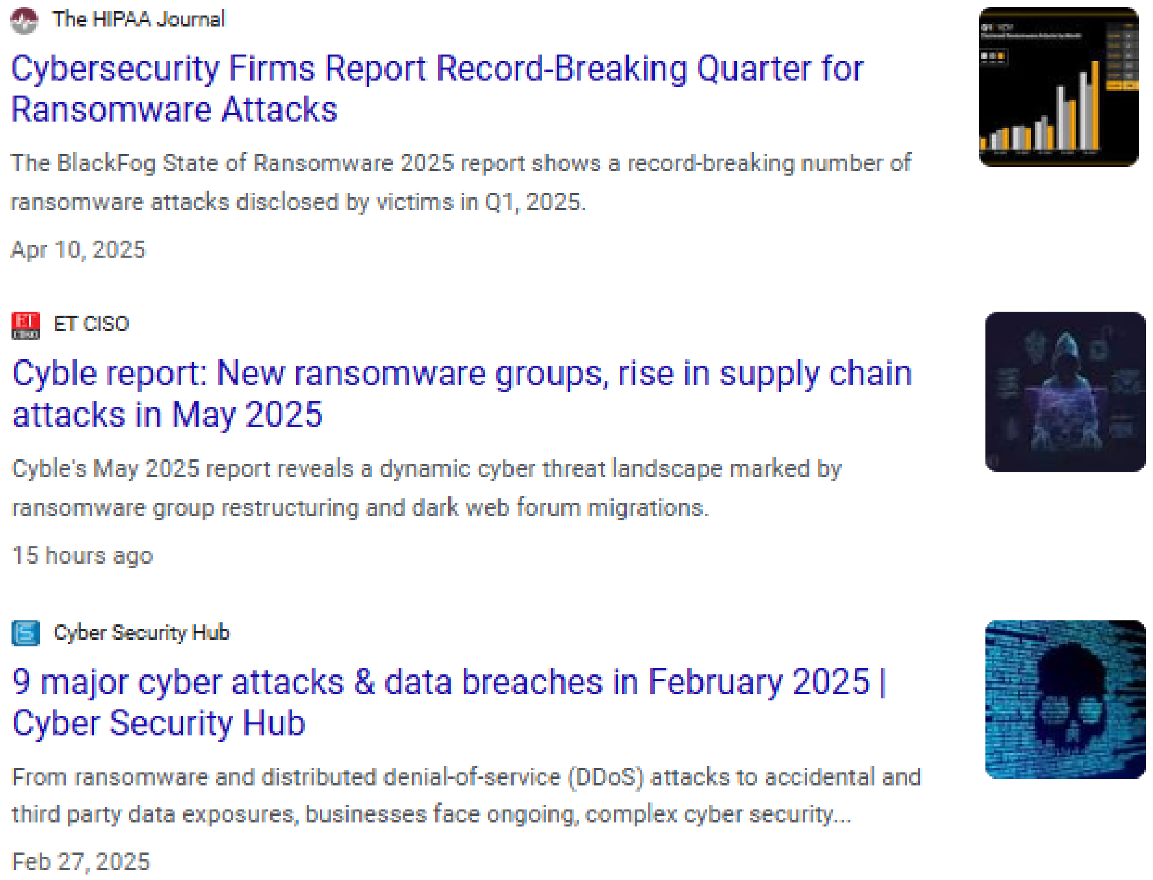
4 days ago

Honeywell

Ransomware Attacks Targeting Industrial Operators Surge 46% in One Quarter, Honeywell Report Finds

Honeywell's 2025 Cybersecurity Threat Report reveals energy, manufacturing and other critical industrial sectors face significant escalation...

3 weeks ago



The HIPAA Journal

Cybersecurity Firms Report Record-Breaking Quarter for Ransomware Attacks

The BlackFog State of Ransomware 2025 report shows a record-breaking number of ransomware attacks disclosed by victims in Q1, 2025.

Apr 10, 2025

ET CISO

Cyble report: New ransomware groups, rise in supply chain attacks in May 2025

Cyble's May 2025 report reveals a dynamic cyber threat landscape marked by ransomware group restructuring and dark web forum migrations.

15 hours ago

Cyber Security Hub

9 major cyber attacks & data breaches in February 2025 | Cyber Security Hub

From ransomware and distributed denial-of-service (DDoS) attacks to accidental and third party data exposures, businesses face ongoing, complex cyber security...

Feb 27, 2025

Operational Disruptions

- CrowdStrike

In July 2024, CrowdStrike released a faulty update to its Falcon Sensor software, causing a global IT outage that impacted approximately 8.5 million Microsoft Windows devices. The update contained a logic error that triggered widespread system crashes, disrupting industries including airlines, healthcare, banking, and government services. The incident cost companies an estimated $5.4 billion. It was not a cyberattack but exposed risks associated with reliance on third party systems. The company faced lawsuits, reputational damage, and implemented new testing and phased rollout processes to prevent future incidents.

Attacks/Outages Caused by Third-Party Providers

Target

The 2013 Target data breach, one of the largest retail breaches in U.S. history, resulted from hackers gaining access to Target’s internal network using stolen credentials from a third-party HVAC vendor.

Microsoft 365 and Azure

AT&T users were unable to access Microsoft 365 and Azure services due to “a third-party Internet Service Provider (ATT) incident that impacted a subset of their customers' ability to connect” according to Microsoft.

ATT

February of 2024, ATT users reported outages for a variety of services, including internet access. AT&T said in a statement that the outage appeared “due to the application and execution of an incorrect process used while working to expand our network.”

CrowdStrike

See previous slide…..

Polling Question 1

Which of the following cyber events was an operational outage?

A. GrubHub
B. CrowdStrike
C. Target
D. ATT

Effective Risk Management Techniques

Risk management techniques should focus on identifying, assessing, mitigating, and monitoring risks to the business. These techniques align with leading frameworks like NIST CSF, ISO 27001, and CIS Controls, addressing modern threats such as ransomware, cloud vulnerabilities, and supply chain attacks.

- Structured Risk Assessment

  Conducting regular, structured risk assessments utilizing leading practices and practices and frameworks can ensure threats, vulnerabilities and impacts are impacts are identified and prioritized.

- Continuous Monitoring

  Utilizing real-time monitoring tools to identify vulnerabilities and threat vectors threat vectors can greatly enhance identification of critical threats such as zero-such as zero-day exploits.

- Security Awareness and Phishing Training

  Train ALL employees how to recognize and deal with cybersecurity threats like threats like phishing, social engineering, vishing. Regularly test the effectiveness effectiveness by performing simulations.

- Incident Response and Recovery

  Develop and test incident response (IR) plans aligned with NIST 800-61 or SANS frameworks. Include playbooks for common scenarios (e.g., ransomware, DDoS).

- Third-Party and Supply Chain Risk Management

  Assess and monitor risks from vendors, cloud providers, and supply chains. Obtain and evaluate compliance reports (SOC, PCI, HIPAA). Use Vendor Risk Management (VRM) tools and enforce contractual security requirements.

- Automated Control Implementation

  Deploy automated technical controls like encryption, endpoint detection and detection and response (EDR), Multi-factor authentication, and automated automated segregation of duties.

- Cyber Insurance

  Purchase cyber insurance to transfer financial risk of breaches, ransomware, or business interruption. Align coverage with risk assessment findings.

- Governance and Policy Alignment

  Establish a risk governance structure with clear roles, policies, and accountability. Align IT risk management with enterprise risk management (ERM) and business goals.

- Regular Audits and Vulnerability/Pen Testing

  Conduct internal and external audits to validate controls, complemented by exercises and penetration testing to simulate real-world attacks.

Most Effective Technique?

- Continuous Monitoring

  The most effective IT risk management technique is continuous threat and vulnerability vulnerability monitoring, coupled with automated response capabilities.

  This approach uses tools like Security Information and Event Management (SIEM) systems (e.g., systems (e.g., Splunk, Microsoft Sentinel) and vulnerability scanners (e.g., Tenable, Qualys) to Qualys) to detect threats, misconfigurations, and vulnerabilities in real time. By integrating threat integrating threat intelligence (e.g., MITRE ATT&CK, CISA alerts) and automating patch patch management or incident response workflows, it minimizes exposure to emerging risks like emerging risks like zero-day exploits or ransomware.

  Its effectiveness lies in early detection and rapid mitigation, reducing the likelihood and impact of and impact of breaches, especially in dynamic cloud and hybrid environments. This technique technique aligns with frameworks like NIST CSF and ISO 27001, making it adaptable and scalable and scalable across industries..

Why do schools and offices have fire drills?

- Practicing for an unexpected event can decrease risk.

- What can organizations do to practice?

  Phishing Exercises:

  1) Assess current capabilities of employees by sending a baseline phishing email test.
  2) Review recent reported phishing emails
  3) Provide initial phishing and cybersecurity training for all employees
  4) Leverage real world phishing examples
  5) Make reporting as simple and easy as possible
  6) Conduct targeted training for repeat offenders

- Phishing Statistics
  - Baseline statistics show 34% of untrained users will click on a phishing email.
  - 90 days of security training and phishing simulations will drop that to 18%
  - Organizations that perform regular phishing exercises reduce the susceptibility to phishing attacks by and average of 86%

Do you have home and auto insurance?

- Does your organization have a cyber insurance policy? policy?

  Insurance against cyber events makes good business sense.

- Effective Cyber Risk Management can lower premiums premiums
  - Implement a recognized security framework – Adopt cybersecurity cybersecurity frameworks like NIST, ISO 27001, or SOC 2 to improve your improve your security posture.
  - Deploy multi-factor authentication – Implement MFA across all critical critical systems
  - Develop and regularly test incident response plans – A well-documented documented incident response plan shows insurers you're prepared to prepared to handle breaches swiftly, thereby minimizing damage and damage and costs.
  - Conduct comprehensive security awareness training – Human error error remains a primary factor in successful cyberattacks. Regular, Regular, engaging security awareness training for all employees reduces employees reduces this risk significantly,
  - Implement proactive monitoring and threat hunting – Moving beyond beyond passive defenses to scan for vulnerabilities and hunt for threats for threats actively demonstrates a mature security approach.

Polling Question 2

Which of the Risk Management techniques is most effective?

A. Risk Assessment
B. Cyber Insurance
C. Automated Controls
D. Continuous Threat and Vulnerability Monitoring

What is Compliance?

com·pli·ance - noun
/kəmˈplīəns/

- The action or fact of complying with a wish or command- they must secure each other's cooperation or **compliance**
- The state or fact of according with or meeting rules or standards- all imports of timber are **in compliance with** regulations

Com·pli·ance (kəm-pl ns) 1. To follow a rule, request, demand, etc.

Common Compliance Frameworks

- SOC (System and Organization Controls) Controls)

  Third-party audit reports, issued by independent, licensed CPAs, licensed CPAs, that assess an organization's internal controls controls related to defined criteria. The reports provide assurance to customers and stakeholders that the organization organization has implemented and maintains effective controls. controls.

- ISO/IEC 27001

  A globally recognized standard for Information Security Management Systems (ISMS) providing a systematic approach to approach to managing sensitive information, focusing on risk on risk assessment, security controls, and continuous improvement.

- NIST Cybersecurity Framework (CSF)

  U.S.-based framework structured around six core functions: Govern, Identify, Protect, Detect, Respond, and Recover. Adopted by organizations globally, especially in critical infrastructure sectors.

- CIS Controls

  Developed by the Center for Internet Security, this framework provides a prioritized set of 18 security controls to protect against common cyber threats. It’s practical for organizations of all sizes, emphasizing actionable safeguards like asset management and incident response.

- PCI DSS

  Payment Card Industry Data Security Standard applies to organizations handling cardholder data. Version 4.0 emphasizes continuous security practices and flexibility in meeting requirements.

- HIPAA

  A U.S. compliance framework for protecting healthcare data. It sets standards for securing Protected Health Information (PHI), requiring administrative, physical, and technical safeguards. Essential for healthcare providers and their business associates.

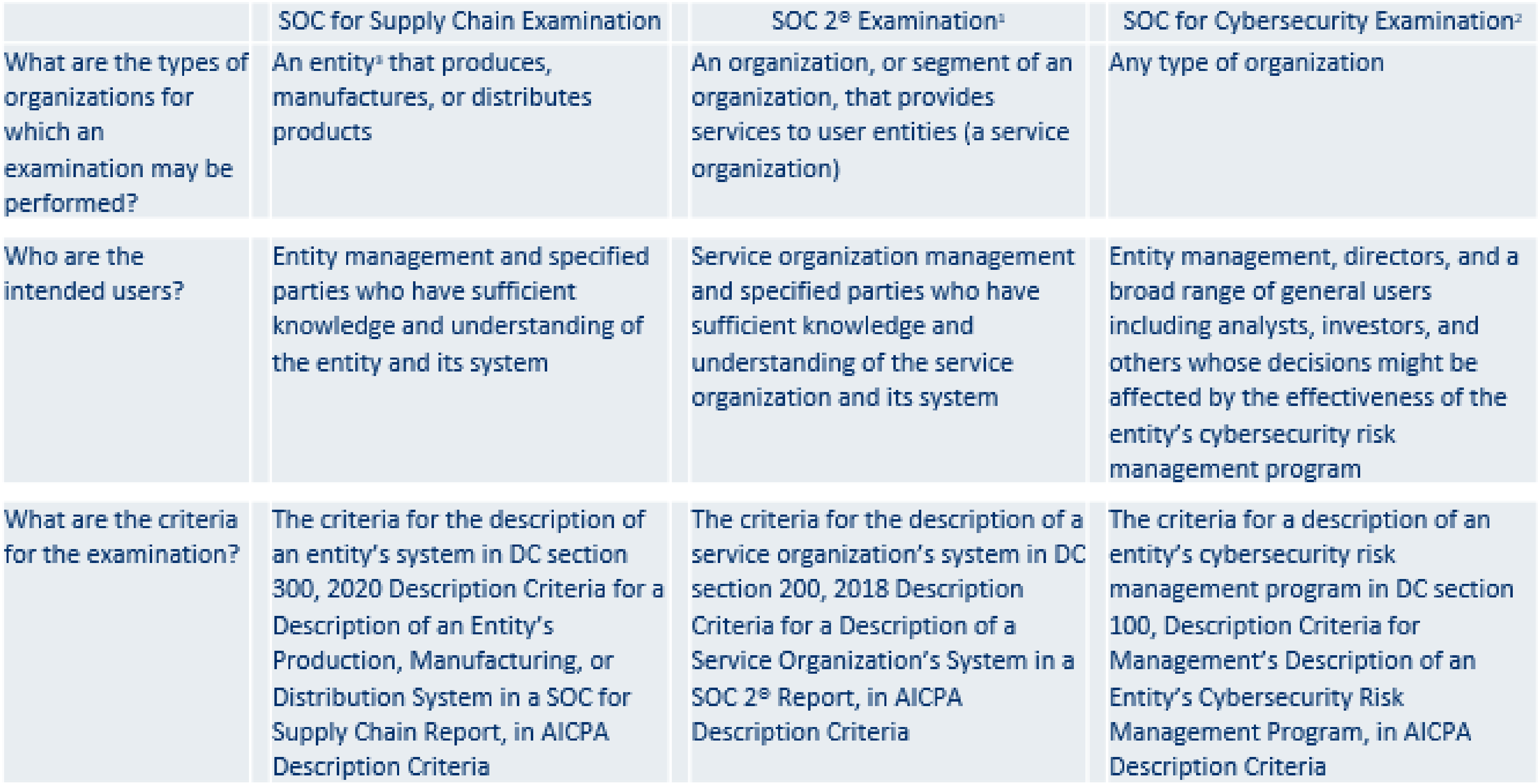
Common Compliance Issues

- Multiple standards and audits based on customer's need.
- Wasted resources scheduling and supporting multiple audits by multiple firms.
- Wasted resources scheduling and supporting audits by customers exercising their "right to audit."
- Lack of clarity and confusion regarding customer expectations.

One SOC, Two SOC, Red SOC, Blue SOC!

- SOC 1®– SOC for Service Organizations: ICFR
- SOC 2® - SOC for Service Organizations: Trust Services Criteria
- SOC 3®— SOC for Service Organizations: Trust Services Criteria for General Use Report
- SOC for Cybersecurity
- SOC for Supply Chain

Common Compliance Issues



	SOC for Supply Chain Examination	SOC 2® Examination[1]	SOC for Cybersecurity Examination[2]
What are the types of organizations for which an examination may be performed?	An entity[3] that produces, manufactures, or distributes products	An organization, or segment of an organization, that provides services to user entities (a service organization)	Any type of organization
Who are the intended users?	Entity management and specified parties who have sufficient knowledge and understanding of the entity and its system	Service organization management and specified parties who have sufficient knowledge and understanding of the service organization and its system	Entity management, directors, and a broad range of general users including analysts, investors, and others whose decisions might be affected by the effectiveness of the entity's cybersecurity risk management program
What are the criteria for the examination?	The criteria for the description of an entity's system in DC section 300, 2020 Description Criteria for a Description of an Entity's Production, Manufacturing, or Distribution System in a SOC for Supply Chain Report, in AICPA Description Criteria	The criteria for the description of a service organization's system in DC section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report, in AICPA Description Criteria	The criteria for a description of an entity's cybersecurity risk management program in DC section 100, Description Criteria for Management's Description of an Entity's Cybersecurity Risk Management Program, in AICPA Description Criteria

Polling Question 3

Which of the following compliance frameworks is intended to evaluate an Information Security Management System?

1) SOC
2) HIPAA
3) ISO/IEC 27001
4) NIST CSF
5) All of the above

Strategies for Success

Back to Basics

- Policies, policies, policies
- Data classification
- Invest in security
- Training

Strategies for Success

Policies

Why are policies important?

- They ensure upper management involvement
- They outline expectations
- Best and least expensive way to communicate
- They are a permanent record of organization's intent
- They enable enforcement

Strategies for Success

Data Classification

- Public or non-classified
- Internal use – only for use inside the organization
- Confidential – should be strongly protected against unauthorized use and disclosure
- Secret – very limited access with very strong protection

Strategies for Success

Invest in Security

- Appropriate security spend depends on data classification
- Understand cost / benefit
- Invest more to protect top secret data
- Invest less to protect public or internal data

Strategies for Success

Train your People

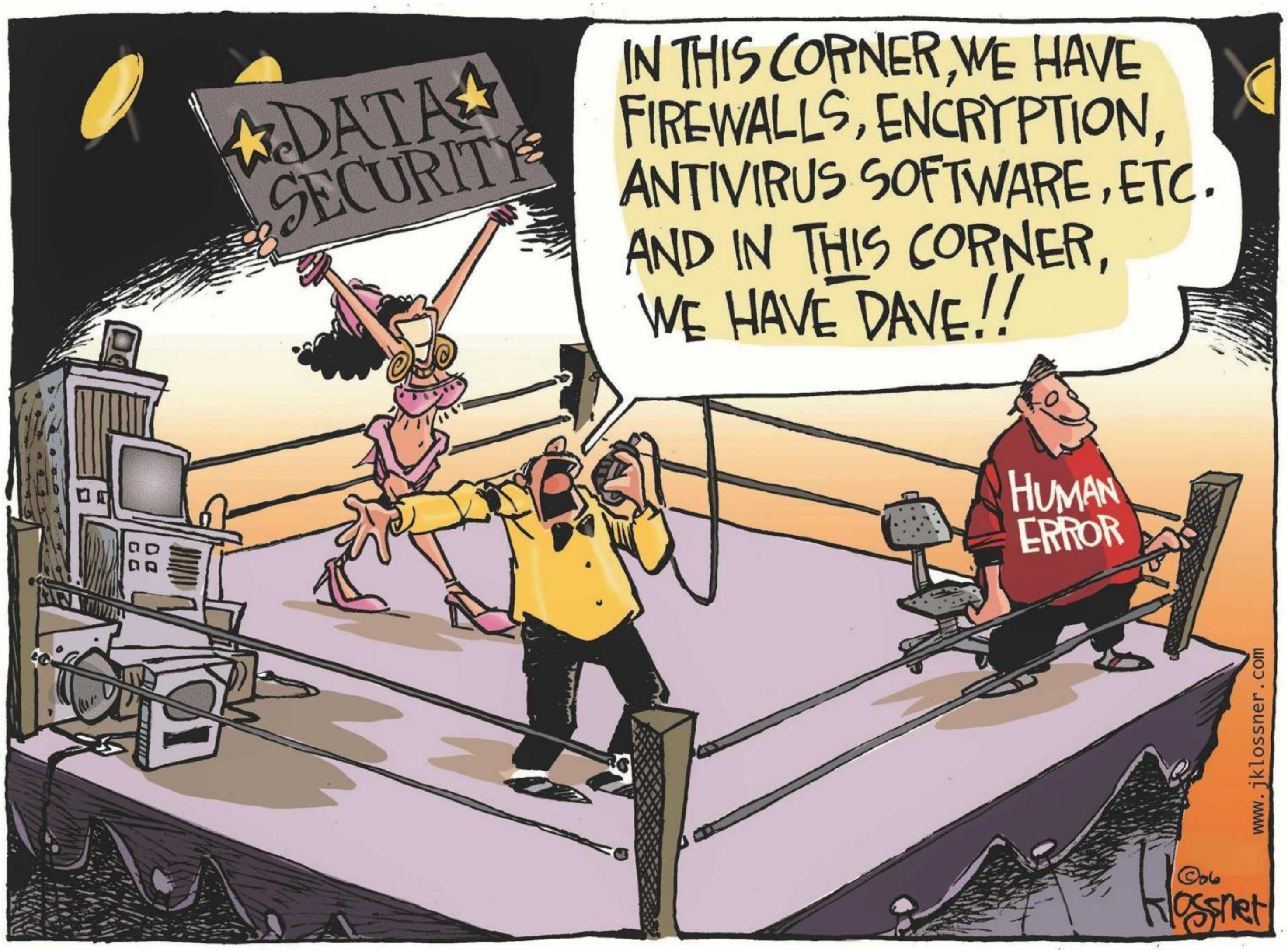
- People are the weakest link
  - Everyone is different
  - Goals and objectives don’t always align
- “Why” is important
  - Not enough to know what the policy is
  - Also need to know why it is in place
  - Lots of examples help reinforce
- Train often
  - People forget so they have to be reminded
  - New threats everyday

Polling Question 4

What is the biggest risk to an organization's cybersecurity?

A. Firewalls
B. People
C. Hackers
D. Lack of cyber insurance

Why is training so important?


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
www.jklossner.com
©06 Klossner

Receiving CPE Credit

- Credit processed within 90 days after the session
  - UHY Colleagues: Credit and certificate available in LCvista
  - External Colleagues: Credit w/ certificate sent from “UHY CPE”
- Credit questions should be directed to CPE@uhy-us.com
- Recordings/materials available 24 hours after the session
  - UHY Colleagues: UHY University
  - External Colleagues: UHY’s event page

UHY

uhy-us.com

Audit | Tax | Advisory | Consulting

"UHY" is the brand name under which UHY LLP and UHY Advisors, Inc. provide professional services. The two firms operate as separate legal entities in an alternative practice structure. UHY LLP is a licensed independent CPA firm that performs attest services. UHY Advisors, Inc. provides tax and business consulting services through wholly owned subsidiary entities. UHY Advisors, Inc. and UHY LLP are U.S. members of Urbach Hacker Young International Limited (UHY International), a UK company, and form part of the international UHY network of legally independent accounting and consulting firms. Any services described herein are provided by UHY Advisors and/or UHY LLP (as the case may be) and not by UHY International or any other member firm of UHYI. Neither UHY International nor any member of UHY International has any liability for services provided by other members.