Welcome to Today's Webinar

Cybersecurity Best Practices for Staffing Agencies

Tues, June 25, 2024, 2 p.m. Eastern time

Please note that the audio will be streamed through your computer—there is no dial-in number. Please make sure to have your computer speakers turned on or your headphones handy.

ASA WEBINARS

ASA American Staffing Association

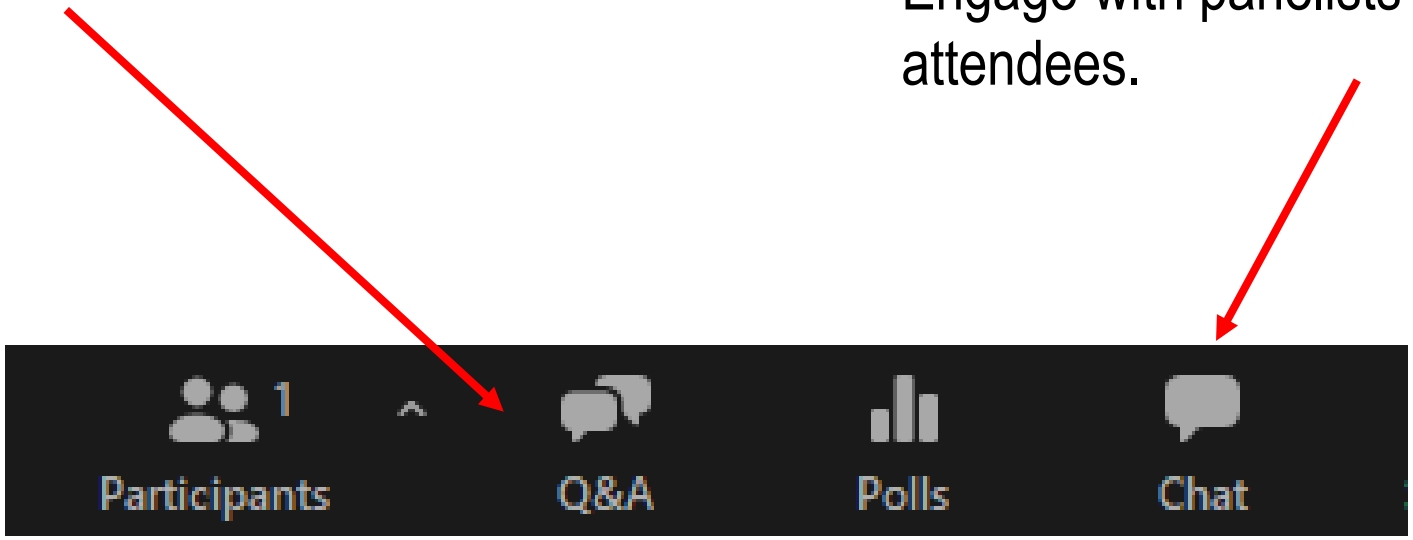
Miller & Chevalier


CC
Show Subtitle
View Full Transcript
Subtitle Settings...
Raise Hand
Q&A
CC
Live Transcript

Ask a Question, Engage With Other Attendees

Q&A
Type your questions for the panel into the Q&A box

Chat
Start a conversation—say hello. Engage with panelists and other attendees.



ASA Certification Continuing Education

Today's webinar qualifies for 1.0 CE hour

- **Live webinar:** NEW as of April 2024—CE credits earned from attending this program are automatically added to your online CE Status within three business days.
- **On-demand viewers**: Submit this earned CE using the online submission form at *americanstaffing.net*.

CSP TSC CSC CHP

- This program is valid for **PDCs** for the SHRM-CP® or SHRM-SCP®.

Activity ID: Activity 24-EDV4Y

SHRM
SHRM-CP | SHRM-SCP
RECERTIFICATION PROVIDER

americanstaffing.net/asa-pro-stacks-programs

Miller & Chevalier

CYBERSECURITY BEST PRACTICES

Ashley Powers
Counsel
apowers@milchev.com

Alex Sarria
Member
asarria@milchev.com

Government Contractor vs. Non-Government Contractor

Government Contractor

- Cybersecurity compliance representations and certifications
- Contractual cybersecurity requirements
- Statutory and regulatory reporting requirements

Non-Government Contractor

- Work might still touch federal funds → require compliance with federal regulations
- Access to and/or storage of information that is valuable to hackers
  - Employee information
    - PII, banking information
  - Information about others gained through performance of contract
    - PII, PHI, CUI

Insight Global LLC

$2.7M False Claims Act settlement

Contract with Pennsylvania Department of Health to provide staffing for COVID-19 contact tracing services

Insight's contract was with PADOH, but PADOH paid Insight, in part, with money from CDC, i.e., federal funds nexus

PADOH contract provided Insight with access to PHI and PII

- Agency alleged that Insight failed to keep PHI and PII confidential and secure
- Failed to encrypt emails with this information
- Staff used shared passwords to access information
- Information was stored and transmitted via Google files that were not password protected

What standards apply?

Government Contractor

- Existing Regulations
  - Executive Order 14028 – Improving the Nation's Cybersecurity
  - CISA
    - Secure by Design Software Framework
  - NIST
    - 800-171 – Handling CUI
  - Agency specific regulations
    - FAR 52.204-21 (Basic Safeguarding of Covered Contractor Information Systems)
    - DFARS 252.204-7021 (Safeguarding Covered Defense Information and Cyber Incident Reporting)
    - CMMC (Cybersecurity Maturity Model Certification) – DoD specific
    - SEC Cybersecurity Incident Disclosure Rule (for publicly held companies)
    - DHS – Safeguarding of Controlled Unclassified Information

Government Contractor, Continued

- Potential future regulations
  - Proposed FAR Rules
    - Cyber Threat and Incident Reporting and Information Sharing
    - Standardizing Cybersecurity Requirements for Unclassified Federal Information Systems
    - Controlled Unclassified Information
    - Supply Chain Software Security
- FAR Part 40 (Information Security and Supply Chain Security)

Government *and* Non-Government Contractors

- Contractual requirements
- Cybersecurity Guidance
  - ISO 27001 – International standard for Information Security Management Systems (ISMS)
    - Considered the “benchmark” for information systems and cyber hygiene
    - ISO Certification is available to private companies
  - NIST 800-53 – list of controls to secure “federal information systems”
    - Even though this is for federal information systems, many states and local, as well as private organizations, use this as a guide for their information systems
    - Organized based on “families” of controls, which include controls for: access control, audit and accountability, awareness and training, incident response, risk assessment, contingency planning, etc.

STRATEGIES TO ENSURE CYBERSECURITY COMPLIANCE

Best Practices

- Read and understand your contract
  - Understand any compliance requirements
  - Understand any reporting requirements
  - Understand what information systems will be involved in contract performance
  - Understand what data/information might be involved in contract performance
    - CUI
    - PII
    - PHI
- Understand any applicable statutory and regulatory requirements
- Follow—or at least benchmark against—ISO 27001

Best Practices, continued

- ISO 27001 adopts a “Plan-Do-Check-Act” model for each element of an Information Security Management System (ISMS).

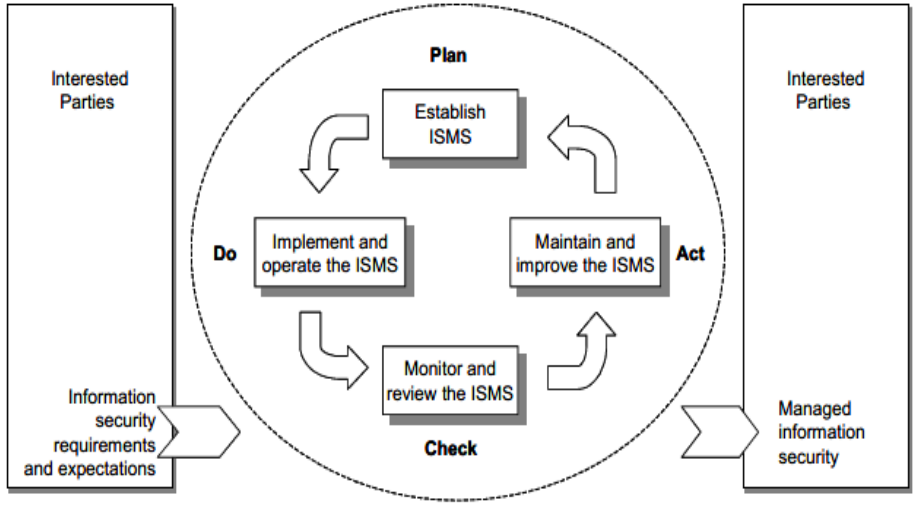


Figure 1 — PDCA model applied to ISMS processes

Plan (establish the ISMS)	Establish ISMS policy, objectives, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization's overall policies and objectives.
Do (implement and operate the ISMS)	Implement and operate the ISMS policy, controls, processes and procedures.
Check (monitor and review the ISMS)	Assess and, where applicable, measure process performance against ISMS policy, objectives and practical experience and report the results to management for review.
Act (maintain and improve the ISMS)	Take corrective and preventive actions, based on the results of the internal ISMS audit and management review or other relevant information, to achieve continual improvement of the ISMS.

Best Practices, continued

- Establish an Information Security Management System (ISMS)
  - Define the scope of the ISMS – take into account characteristics of the business, the organization, its assets, and its technology
  - Define an ISMS policy
    - Includes a framework for objectives and principles for information security
    - Takes into account business and legal/regulatory requirements, as well as contractual obligations
    - Aligns with organization's risk tolerance
    - Establishes criteria against which risk will be evaluated
    - Approved by management
  - Define the risk assessment approach of the organization
    - Develop criteria for accepting risk and identify acceptable levels of risk
  - Critical part of the above → identifying organization's risks
    - Identify assets within the ISMS and owners of these assets
    - Identify threats to those assets
    - Identify vulnerabilities that might be exploited by these threats
    - Identify impacts of loss of confidentiality, integrity, etc, to those assets

Establishing an ISMS, continued

  - Identify and evaluate options for treatment of risks
    - Apply appropriate controls
    - Accept risks consistent with policies and criteria for accepting risk
    - Avoid risks
    - Transfer risks to other parties, i.e., insurers, suppliers
- Implementing and operating ISMS
  - Formulate and implement risk treatment plan
  - Define how to measure effectiveness of controls
  - Implement training and awareness programs
  - Manage operation and resources for ISMS
  - Implement procedures for detecting and responding to security incidents

Establishing an ISMS, continued

- Monitor and Review the ISMS
  - Execute monitoring procedures
  - Undertake regular reviews of effectiveness of the ISMS
  - Measure effectiveness of controls to verify metrics met
  - Periodically review risk assessments
  - Conduct internal ISMS audits
  - Regular management review of ISMS
  - Update policies and procedures
  - DOCUMENT DOCUMENT DOCUMENT
    - Establish procedures for approval, review, control, and retention of associated documents

Establishing an ISMS, continued

- Management Responsibility
  - Establish ISMS policy, objectives, and plans
  - Establish roles and responsibilities for information security
  - Top—down messaging
  - Provide sufficient resources for effective ISMS framework
  - Ensure that ISMS procedures and policies are followed
  - Conduct review of the ISMS

Examples of Administrative Safeguards

- Management
  - Information Security
  - Incident Response
  - Disaster Recover
- End-users
  - Acceptable Use
  - Mobile Device
  - Password
- Others
  - Encryption
  - Network security

POTENTIAL CONSEQUENCES OF CYBERSECURITY BREACHES

Potential Cybersecurity Issues and Consequences

- Potential Issues
  - Providing deficient cybersecurity products or services
    - This includes failing to comply with contractual data privacy requirements
  - Misrepresenting cybersecurity compliance
  - Failing to monitor or report cybersecurity incidents as required by contract
- Potential Consequences
  - Breach of contract or warranty lawsuit
  - Data / privacy protection litigation
  - Government contractors
    - Termination for default
    - Office of Inspector General
    - Suspension or Debarment
  - Department of Justice – Civil Cyber Fraud Initiative

Recent Cybersecurity Judgments and Settlements

- 6/17/2024 – Guidehouse - $11.3M
- 5/1/2024 – Insight Global - $2.7M
- 9/5/2023 – Verizon Business Network Services - $4M
- 3/14/2023 – Jelly Bean Communications Design - $293,771

CYBERSECURITY RESOURCES

Resources and training

- NSA (https://www.nsa.gov/Cybersecurity/)
- DoD (https://public.cyber.mil/)
- NIST (https://www.nist.gov/cybersecurity)
- CISA (https://www.cisa.gov/resources-tools)
- DOJ (https://www.justice.gov/jmd/cybersecurity-services)
- FBI (https://www.fbi.gov/investigate/cyber)

QUESTIONS?

Miller & Chevalier

ASA Certification Continuing Education

Today's webinar qualifies for 1.0 CE hour

- **Live webinar:** NEW as of April 2024—CE credits earned from attending this program are automatically added to your online CE Status within three business days.
- **On-demand viewers**: Submit this earned CE using the online submission form at *americanstaffing.net*.

CSP TSC CSC CHP

- This program is valid for **PDCs** for the SHRM-CP® or SHRM-SCP®.

Activity ID: Activity 24-EDV4Y

SHRM
SHRM-CP | SHRM-SCP
RECERTIFICATION PROVIDER

You will now be redirected to a brief survey