SESSION ID: AST1-R02

CYBERSECURITY CAPABILITY READINESS: NECESSARY CONVERSATIONS, NEXT STEPS

MODERATOR: Matt Loeb, CGEIT, FASAE, CAE
Chief Executive Officer, ISACA

PANELISTS:

E. Douglas Grindstaff
Global New Business and Market Development, CMMI Institute

Rich Licato, CISA, CRISC, CGEIT
Chief Information Security Officer, ARC

Tammy Moskites, CISM, ITIL
Managing Director, Accenture Security, Accenture

Mike Raeder, CISM, CISA
Chief Information Security Officer, Orbital ATK
Current challenges in the cybersecurity workforce

3 in 5 organizations have unfilled cybersecurity/information security positions.

- 59% of positions are unfilled.

Respondents who say their organization can fill open positions in 3 months or less:

- 45% in 2018
- 54% in 2017
- 52% in 2016

Top two gaps in today’s security professionals:

- 39% of respondents say inability to understand business needs
- 33% of respondents say technical skills
Cybersecurity Capability Readiness: Necessary Conversations, Next Steps

State of Cybersecurity Research 2018

Aligning Security Strategy with Organizational Objectives:

84%  79%  75%
2018  2017  2016
Discussion Points:

- What is your total cost of ownership around security controls?
- Landscape level set:
  - What is cybersecurity capability?
  - What is cybersecurity resilience?
  - What is cybersecurity maturity?
From Compliance to Resilience: Is There a Copernican Shift?
Cybersecurity Capability Readiness: Necessary Conversations, Next Steps

Cybersecurity Readiness & Resilience

**SecOps:** SecOps describes effective integration of security and IT/OT operations in **three key areas:**
- Mission priorities & dependencies
- Threat information
- Secure and available technology

**Capability Maturity:** Focusing on **risk-based capabilities** is foundational to building resilience

**Workforce Readiness:** 60% of all attacks were carried out by insiders. 75% involved malicious intent. The **workforce** is our greatest point of vulnerability and opportunity.
Cybersecurity Assessment Approach and Solution

- **STANDARDIZED MATURITY**: Defines maturity for people, process and technology; includes hygiene; enables industry benchmarking.
- **ORGANIZATION-WIDE, RISK-BASED**: Defines the organization’s risk profile and sets maturity targets.
- **ROADMAP DEVELOPMENT**: Provides risk-based prioritization of gaps in capabilities, maturity to support roadmap development, investment options.
- **COMPLIANCE VIEWS**: Provides views into compliance with industry-standard COBIT 5, ISO27001, NIST CSF, CMMI Threat Kill Chain, etc.
Discussion Points:

- How does maturing cybersecurity capabilities prepare organizations for a dynamic threat landscape?
- How does building cybersecurity capabilities build Board confidence in their cybersecurity program?
- How does minimizing risk enable employee and leadership confidence in business performance and outcomes?
Questions from the audience

Thank you!