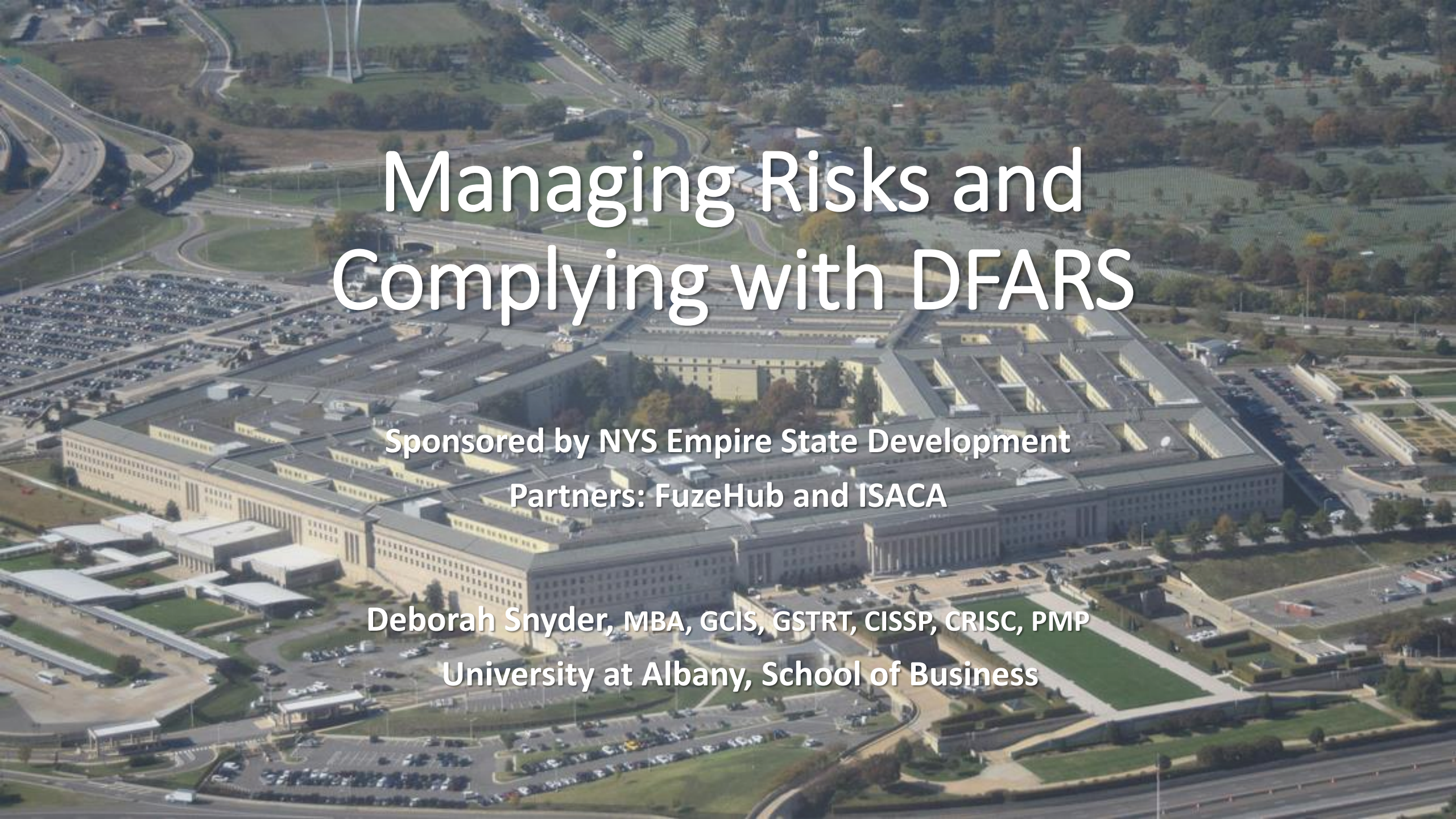

Managing Risks and Complying with DFARS

Sponsored by NYS Empire State Development

Partners: FuzeHub and ISACA

Deborah Snyder, MBA, GCIS, GSTRT, CISSP, CRISC, PMP

University at Albany, School of Business

Cybersecurity Risk is a Strategic Matter

- Part of enterprise risk management
- Supports business goals and objectives
- Protects valuable physical and digital assets
- Cyber crimes are on the rise
- Impact from incidents and data breaches can be severe
- Consequences of failure can affect the bottom line; ruin a business

Cyber Threat Landscape

- Attacks growing in number and sophistication
- Financial loss increased 58% over 2 years (2018 Global State of Information Security Survey, PWC)
- Less than half (42%) of all organizations are confident in their risk management strategies (ATT Cyber Security Insights, Vol. 8)
- 64% of breaches involved weak controls (Verizon Data Breach Investigation Report)
- Only 44% of corporate boards actively participate in their organization's overall security strategy (PWC)

Economic Impact

Global average cost of a data breach — $3.62 million

Global cost of cybercrime **~$600 billion** — about .8 percent of global GDP

(2019 Ponemon Institute Study)

Cyber Incident Trends — Manufacturing

- Breaches — financially driven; cyber-espionage is still a strong motivator
- Most begin with phishing attacks
- Stolen credentials and web applications are most common hacking vectors
- Basic security measures would have mitigated risk

(2019 Verizon Data Breach Investigations Report)

Cyber Risks — Manufacturing

- New models of operation and technologies
- Hyper-connectivity of industrial devices, cyber-physical systems and automation
- Protecting data/intellectual property from unauthorized access, theft, damage
- Operational impact
- Regulatory compliance, legal implications
- Public expectations of trust, service/product quality
- Partnerships, third-party risk

Data and Digital Trust

- Information is the lifeblood of business
- Digital business models mean more data collected, generated and shared
- Data governance, security, privacy and ethics are essential

Cybersecurity Frameworks

- Effective program governance and reporting
- Structured risk management approaches to identify and assess risk
- Realistic recommended control practices, based on most common and impactful scenarios
- Business value — prioritized, proactive cyber defense strategies and investments

Risk Management

Holistic approach

- Frame strategy
- Assessment
- Response
- Monitor

Objectives:

- Identify and understand existing and emerging risks
- Support decision-making
- Prioritize investments and mitigate vulnerabilities

Risk Assessments

Process steps:

1. Prepare
2. Conduct the assessment
3. Communicate risk
4. Maintain and Monitor

Risk analysis considers:

- Assets
- Threats (source & event)
- Vulnerabilities
- Likelihood
- Impact
- Controls (existing; cost/value)

Further Guidance

- **DFARS –** DEFENSE FEDERAL ACQUISITION REGULATION SUPPLEMENT https://www.dcaa.mil/Home/DFARS
- **NIST 800-30,** Guide for Conducting Risk Assessments https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf
- **NIST 800-39,** Managing Information Security Risk: Organization, Mission, and Information System View https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf
- **NIST 800-171r1**, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf
- **NIST 800-171A,** Assessing Security Requirements for Controlled Unclassified Information https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171A.pdf

Contact

Deborah Snyder, MBA, GCIS, GSTRT, CISSP, CRISC, PMP
dasnyder@albany.edu

UNIVERSITY AT ALBANY
State University of New York

CENTERS FOR EXCELLENCE

The School is home to the Center for Advancement & Understanding of Social Enterprises; the Center for Forensics, Analytics, Complexity, Energy, Transportation and Security; the Center for Institutional Investment Management and the Institute for Financial Market Regulation.