Presentation

Workforce Development through Cybersecurity & Project Management Certifications

Dr. Jo-Ann Rolle,
Mr. Jerry Perone, &
Mr. Leo Dregier III

Moderator

Dr. Jo-Ann Rolle,
Consultant

Agenda

- Introduction of panelist
- Overview of Cybersecurity Workforce Development & Planning
- Short presentation and discussion by each panelist on cybersecurity & project management training landscape
- Questions and perspectives for the future
- Audience Q & A

3

Moderator

Dr. JoAnn Rolle

Throughout the last decade, Dr. Rolle has served in C level positions in both private and public institutions delivering new programs, increased revenues and improved brand recognition.

Dr. Rolle earned her Bachelors of Business Administration from the University of Miami, a Master's from Southern Illinois University in Economics, and a Ph.D. in Economics from Howard University. Dr. Rolle is a former administrative fellow of Harvard University Dr. Rolle Can be reached at jdrolle@me.com.

Presenter

Jerry Perone:

Mr. Perone is a seasoned executive, an entrepreneur, author, speaker and consultant. He has been responsible for all aspects of business and project-program management (P/PM); has been on the Board of seven companies, as well as starting and operating several of his own businesses. He is the author of the book "Entrepreneur Boot Camp" and the host of WBZS Business Radio's Weekly Show by the same name. Mr. Perone earned his BS in Electronic Technology from the University of Dayton, and a MBA in Finance & Accounting. Mr. Perone can be reached at jerry.perone@verizon.net.

Presenter

Mr. Leo A. Dregier III:

Leo has been a principal at the computer security firm The Security Matrix, LLC since 1995. Leo has held over 40+ career certifications relating to computer networking, information assurance, forensics, project management, and cyber security. He has helped thousands of IT professionals achieve their certifications online at TheCodeOfLearning.com and maintains an evaluation level above 90+. Leo has also created FindRealEstateHelp.com, which is a real estate problem solving and investment company. You can contact him at LeoDregier.com

Cyber Workforce Development

Cybersecurity Workforce Development =

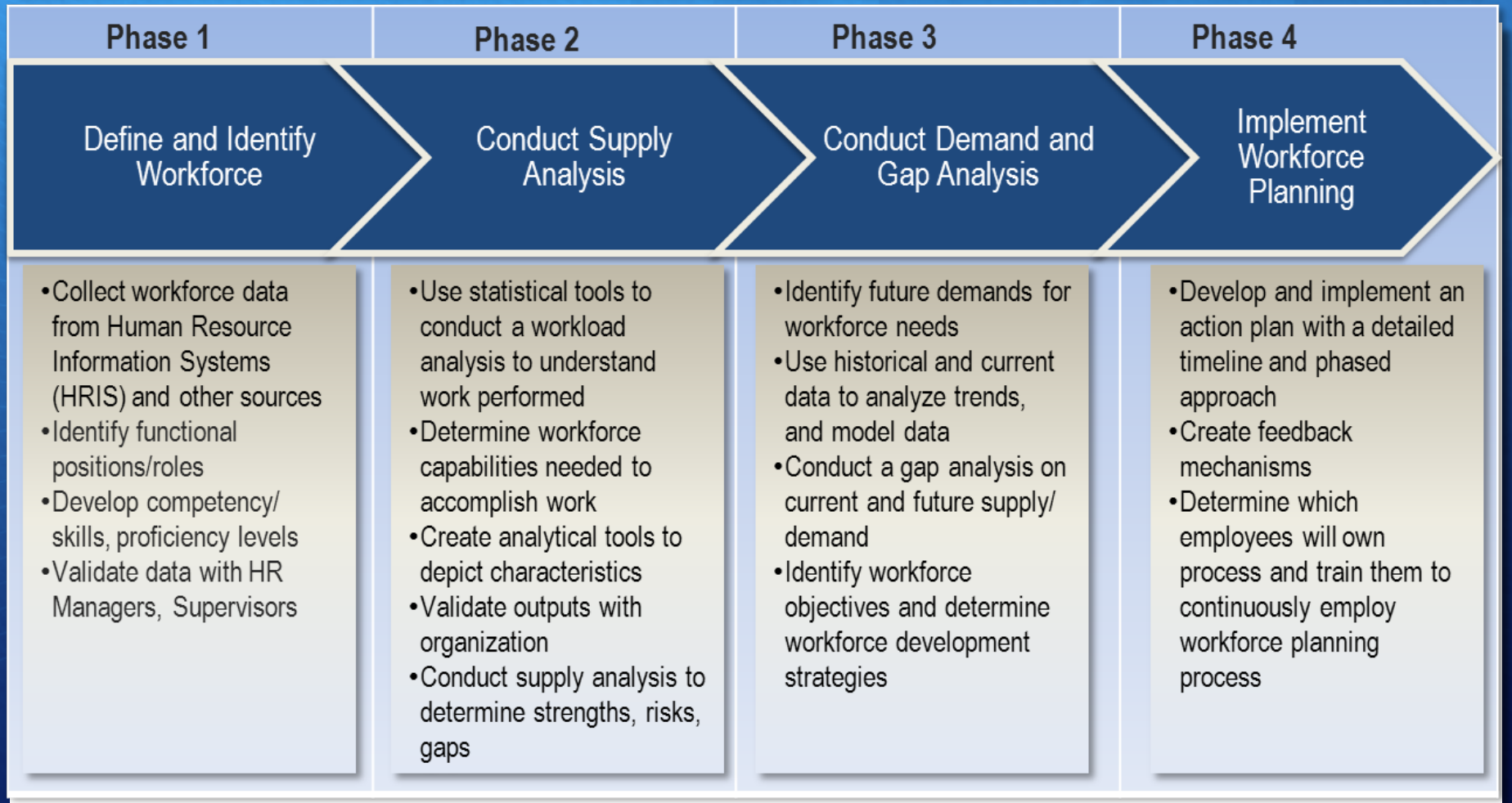
Workforce Assessment + Workforce Planning +Professional Development

1. Cybersecurity Skills Assessment & Analyses
   - Homeland Security Advisory Council Cyberskills Task Force Report Fall 2012
   - National Survey - Federal IT professionals – Fall 2012

2. Cybersecurity Workforce Planning requires shared vision and performance management. (http://niccs.us-cert.gov/training/workforce-development)

3. Cybersecurity Education,Training & Support (http://niccs.us-cert.gov/training/training-home)
   - National Cybersecurity framework provides additional support.
   - NICCS Education & Training catalog available in 2013.
   - Cybersecuirty Professional Development career roadmaps available in 2013.

Workforce Planning Chart



(http://niccs.us-cert.gov/careers/workforce-planning)

Presenter

Mr. Jerry Perone,
CEO National Management Center

Workforce development through cybersecurity & project management

Position– project management

Document Research was performed across various organizations regarding cybersecurity in order to assess the importance given to project management. Our conclusion is that

Project Management has not been sufficiently elevated in order to achieve the desired or required Workforce Development Objectives.

Note: The phrase Project Management is used in this presentation to mean project, program and portfolio management

Basis of position

- Today's business environment is constantly and rapidly changing.
- If businesses are to survive, they must change while they operate.
- The Workforce simultaneously operates and manages the processes of business and also performs and manages change-related activities (As-is State to the To-Be State)
  - Process Management for operations
  - Project Management for change
- Virtually all business today involves a person or people interacting with information technology at some level thereby exposing the business to an unacceptable level of risk exposure.
- Making changes to improve the Organizational Cybersecurity Maturity can lower the risk exposure to an acceptable level
- Project Management is required to raise the Cybersecurity Maturity.

Recommended actions

The cybersecurity objective should be to raise the organization cybersecurity maturity level via program and project management.

- Establish a Cybersecurity Program Office by staffing with experienced program management & Cyber personnel.
- Identify appropriately skilled personnel to serve as a Cyber Maturity Management Team (steering committee) overseeing the Cyber Maturity Initiative and the projects in its portfolio.
- Design a set of metrics which will provide visibility and guidance.
- Charter a project to identify the As-is State and To-Be State for a mature cybersecurity organization.

Recommended actions (continued)

- Develop a transformation program management plan to bring the organization from the As-is to the To-be State.
- Execute the transformation plan by building a matrix managed, projectized cyber team
- Transformation must include a comprehensive education and training program with periodic assesments in order to measure knowledge, retention, application based on the Kirkpatrick Evaluation Model.
- Communications is critical in an organizational transformation plan. Develop a detailed well thought out communications plan using P.R. personnel when needed.

Contact info

For any questions please email

jerry.perone@verizon.net

Thank you very much

Presenter

Mr. Leo Dregier III,
CEO The Security Matrix

Cone of Learning

After 2 weeks we tend to remember		Nature of Involvement
90% of what we say and do	Doing the Real Thing	Active
	Simulating the Real Experience	
	Doing a Dramatic Presentation	
70% of what we say	Giving a Talk	
	Participating in a Discussion	
50% of what we hear and see	Seeing it Done on Location	Passive
	Watching a Demonstration	
	Looking at an Exhibit Watching a Demonstration	
	Watching a Movie	
30% of what we see	Looking at Pictures	
20% of what we hear	Hearing Words	
10% of what we read	Reading	


OPERATE AND MAINTAIN
SECURELY PROVISION
PROTECT AND DEFEND
OVERSIGHT AND DEVELOPMENT
ANALYZE
INVESTIGATE
COLLECT AND OPERATE

SAMPLE JOB TITLES (CONTINUED)

Systems Security Architecture - Develops system concepts and works on the capabilities phases of the systems development lifecycle; translates technology and environmental conditions (e.g., law and regulation) into system and security designs and processes.

- Information Assurance (IA) Architect
- Information Security Architect
- Information Systems Security Engineer
- Network Security Analyst
- Research & Development Engineer
- Security Architect
- Security Engineer
- Security Solutions Architect
- Systems Engineer
- Systems Security Analyst

Technology Research and Development - Conducts technology assessment and integration processes; provides and supports a prototype capability and/or evaluates its utility.

- Capabilities and Development Specialist
- Chief Engineer
- Research & Development Engineer

Systems Requirements Planning - Consults with customers to gather and evaluate functional requirements and translates these requirements into technical solutions. Provides guidance to customers about applicability of information systems to meet business needs.

- Business Analyst
- Business Process Analyst
- Computer Systems Analyst
- Human Factors Engineer
- Requirements Analyst
- Solutions Architect
- Systems Consultant
- Systems Engineer

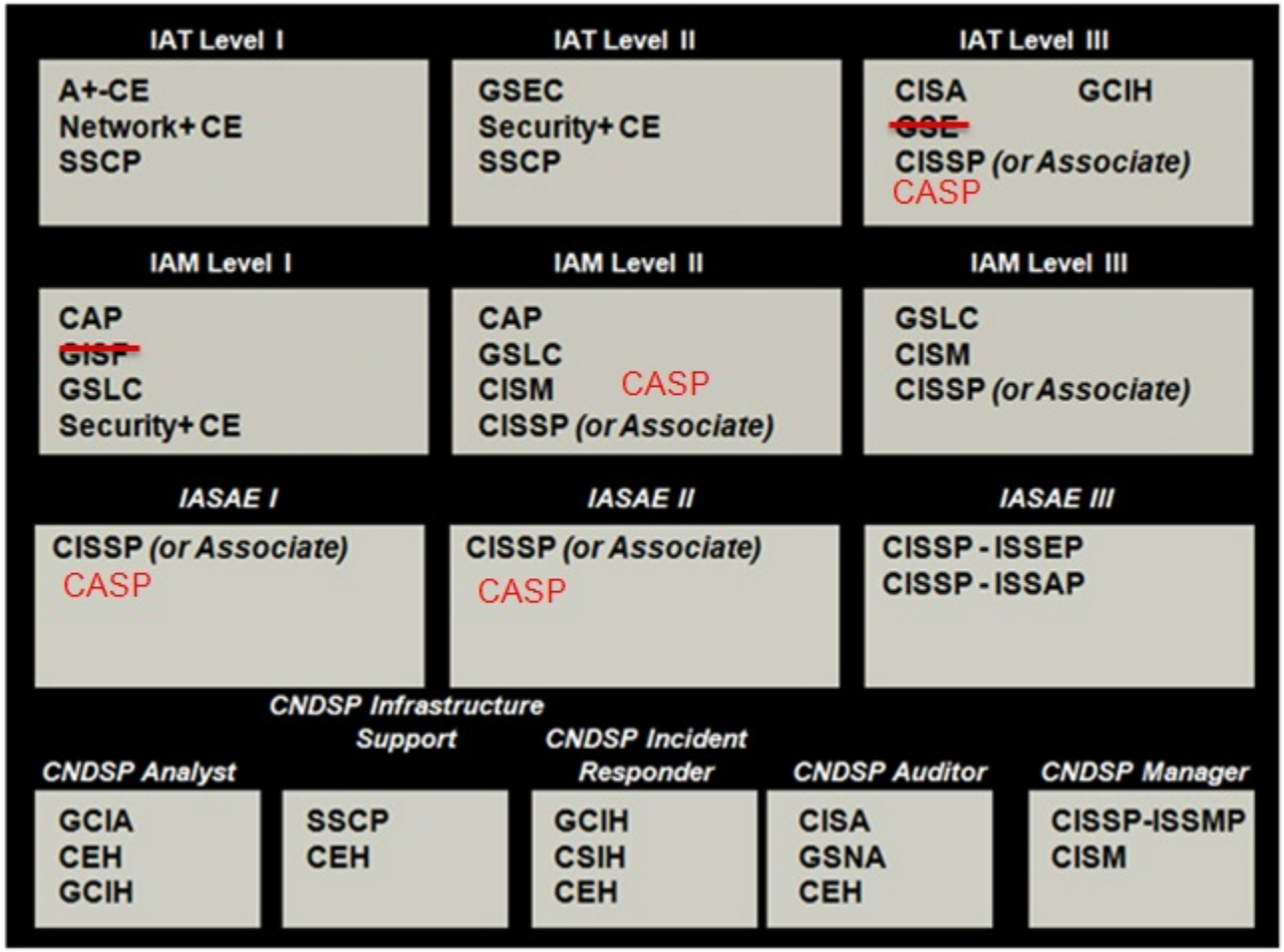
Test and Evaluation - Develops and conducts tests of systems to evaluate compliance with specifications and requirements by applying principles and methods for cost-effective planning, evaluating, verifying, and validating of technical, functional, and performance characteristics (including interoperability) of systems or elements of systems incorporating information technology (IT).

- Application Security Tester
- Information Systems Security Engineer
- Quality Assurance (QA) Tester
- Research & Development Engineer
- Research & Development Research Engineer
- Security Systems Engineer
- Software Quality Assurance (QA) Engineer
- Software Quality Engineer
- Systems Engineer
- Testing and Evaluation Specialist

TASK / KSA

ID	Statement	Competency
19	Knowledge of computer network defense (CND) and vulnerability assessment tools, including open source tools, and their capabilities	Computer Network Defense
58	Knowledge of known vulnerabilities from alerts, advisories, errata, and bulletins	Information Systems/Network Security
63	Knowledge of information assurance (IA) principles and organizational requirements that are relevant to confidentiality, integrity, availability, authentication, and non-repudiation	Information Assurance
69	Knowledge of Risk Management Framework (RMF) requirements	Information Systems Security Certification
77	Knowledge of current industry methods for evaluating, implementing, and disseminating information technology (IT) security assessment, monitoring, detection, and remediation tools and procedures, utilizing standards-based concepts and capabilities	Information Systems/Network Security
88	Knowledge of new and emerging information technology (IT) and information security technologies	Technology Awareness
121	Knowledge of structured analysis principles and methods	Logical Systems Design
128	Knowledge of systems diagnostic tools and fault identification techniques	Systems Testing and Evaluation
143	Knowledge of the organization's enterprise information technology (IT) goals and objectives	Enterprise Architecture
183	Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes	Information Assurance
203	Skill in identifying measures or indicators of system performance and the actions needed to improve or correct performance relative to the goals of the system	Information Technology Performance Assessment
942	Knowledge of the organization's core business/mission processes	Organizational Awareness

Table AP3.T2. DoD Approved Baseline Certifications



Additional Changes??

- How will distance learning change?
- How will onsite learning change?
- How will funding change?

- Other challenges?

Summary & Questions to the Panelist

Audience

Q & A