Enterprise Computing Conference (ECC) Workshop

Alma R. Cole, CISSP, EACOE
VP Cybersecurity
Robbins Gioia

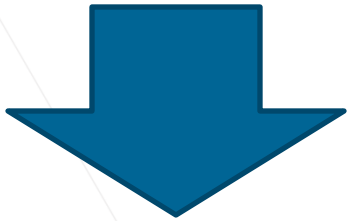
6/15/2015

Current Cybersecurity Challenges

- Increasing dependence on Information Technology
- Increasingly greater complexity in systems and interconnections
- Shortage of qualified cyber security personnel
- Wide spread in security requirements, system architectures, and risk tolerance
  - One size does not fit all

Attacks Constantly Evolving

- Increase in cyber threat actor skills, organization, and motivation
- Increasing frequency and intensity of attacks
- Ineffectiveness of traditional security tools due to constantly changing attacker Tactics, Techniques, and Procedures



- Increases in data breaches and intrusions

Needs for turning the tide against cyber intrusions

ROBBINS GIOIA

1. Grow and develop technical cybersecurity practitioners
   - "Cyber ninjas wanted"
   - Understand hacker methods and how to use security technologies to detect and prevent them
   - Developing skilled analysts capable of finding the new attacks through use of network traffic analysis, malicious code reverse engineering, intrusion forensics, and etc.
   - Understand cyber vulnerabilities and how to remediate them

Needs for turning the tide against cyber intrusions (cont.)

ROBBINS GIOIA

2. Develop cyber-savvy business professionals

- "To defend the organization you need to understand the organization"
- Develop Security Enterprise Architecture experts and methods to assure understanding, alignment, and context
- Ensure that cyber risk and security requirements to support business objectives can be prioritized and effectively communicated to business leadership

Needs for turning the tide against cyber intrusions (cont.)

ROBBINS GIOIA

3. Develop next generation tools and platforms

- Security programs and tools should be designed to plan for failure
- Apply organizational context, cyber intelligence, and trends to make sense of the data
- Develop systems capable of sharing cyber information at machine speed

Summary Thoughts

- Cybersecurity risk is at an all time high due to increasing dependency on IT, complexity of systems, and sophistication of cyber threats
- The next generation of cyber professionals must not only have the correct technical knowhow but must understand the organization and the language of business to adequately align security programs, optimize security tools, and communicate risk and requirements to business leaders
- Design security programs to expect failure but learn from it adapt to changing attacks
- Develop security tools to make sense of the noise and to utilize and share cybersecurity information