

# Paradigm of Dependable Security



## Speaker Benefits:

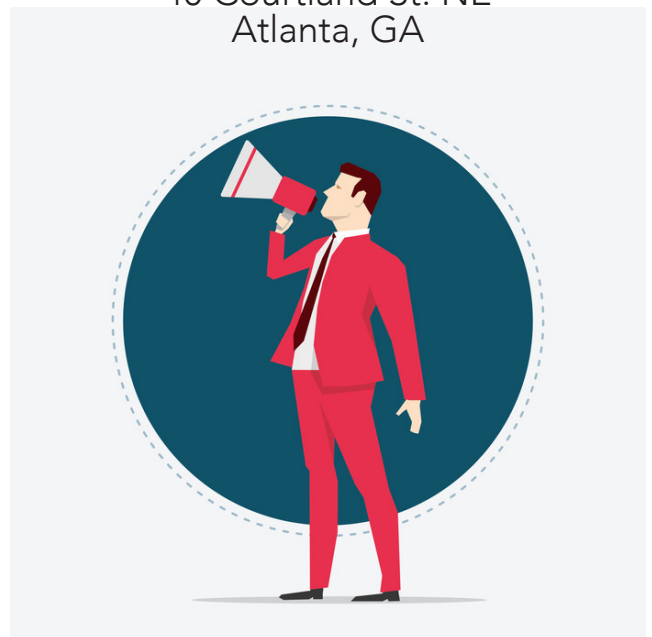
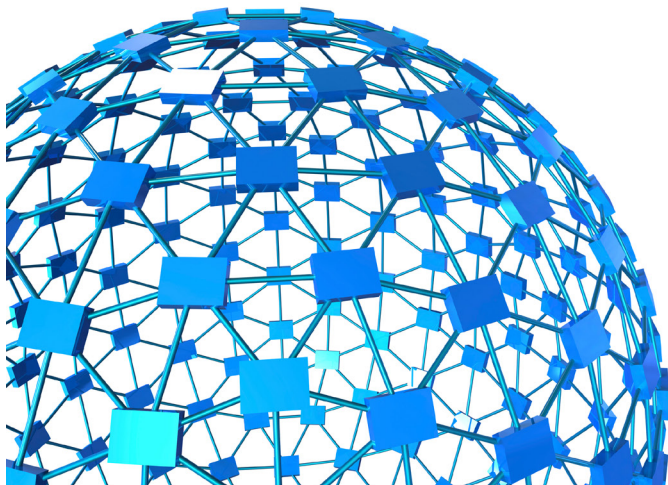
- Expanded business base (Clients and professional peers)
- Heightened professional visibility and corporate exposure.
- Widened industry lecture experience.
- Free conference pass and promotion of your participation in print and electronic media

## Call for Speakers

Deadline for Submission:  
September 1, 2017

Conference Date:  
November 15, 2017

Loudermilk Conference Center  
40 Courtland St. NE  
Atlanta, GA



**ISSA**  
METRO ATLANTA CHAPTER

We are now accepting proposals for speaker presentations for the 2017 Paradigm of Dependable Security Information Security Conference. The theme for the conference is to demonstrate how the security posture of many organizations can be jeopardized by the lack of basic security practices. As security practitioners, we can assist in ensuring that our companies are not overlooking these fundamental building blocks of a solid security program. As such the impetus of each presentation should focus on how the neglect of fundamental security best practices can wreck havoc for any corporation.

Please ensure you are available to speak on the date above before submitting a proposal. All abstracts are reviewed on the basis of applicability, originality, conference needs and speaker qualifications.

Please submit your presentation, lecture abstracts, the speakers' professional bio, and appropriate contact information for follow-up by email to:

[conference@gaissa.org](mailto:conference@gaissa.org).

In the body of the email, address the following:

1. Classify your presentation as: Management, Technical or Compliance Track
2. Classify your presentation as: Beginner, Intermediate or Advanced

The following areas have been identified to have the most interest; however, a submission outside of these areas will be considered as long as the theme of the presentation adheres to the theme of the conference of "Paradigm of Dependable Security".

#### I. Management Tracks:

- Information Security and Risk Management
- Legal, Regulations, Compliance and Investigations
- Security Architecture and Design
- Business Continuity and Disaster Recovery Planning
- Telecommunications and Network Security

The Management track addresses issues impor-

tant to managers such as policies, controlling costs/budget, strategic solutions, hiring and retention, future direction of security and regulatory impact, legal issues, business continuity, disaster recovery, standards such as NIST, ISO, Certification and Accreditation (C&A), Risk management etc.

#### II. Technical Tracks:

- Telecommunications and Network Security
- Cryptography
- Information Security and Risk Management
- Application Security
- Security Architecture and Design

The Technical track may have demonstrations and hands on training on topics such as: How attacks occur; Tools to detect, block or remediate threats; Hardening operating systems (Unix/Linux and Windows); Security controls; How to test security controls; End point security; Computer forensics, Web application attacks (SQL Injection, XSS/CSRF); Application Security. The sessions will be at the following levels –Beginners, Intermediate, Advanced.

#### III. Compliance Tracks:

- Legal, Regulations, Compliance and Investigations
- Information Security and Risk Management
- Telecommunications and Network Security
- Security Architecture and Design
- Operations Security

The Compliance track covers specific compliance issues and tools, such as PCI, IT Governance, Auditing frameworks, SCAP, Automated audit and audit reduction tools, etc.

**PLEASE NOTE:** The intent of these sessions is to educate the Information Security and Assurance professional. **Every presentation must be vendor neutral and not a sales presentation.** Sales and promotional opportunities are available through sponsorship and participation in the vendor gallery.