CALL FOR SPEAKERS
INFOSECURITY/ISACA NORTH AMERICA
EXPO AND CONFERENCE 2019

Infosecurity® and ISACA® are both dedicated to promoting knowledge and networking opportunities for information security professionals. As Europe's leading information security event organizer, Infosecurity (Reed Exhibitions) looks to bring the global infosecurity community together in person, in print and online. ISACA is a trusted leader in education, training, certification and conferences for information systems, cybersecurity and business professionals worldwide.

In 2019, Infosecurity and ISACA will collaborate in hosting a must-attend event that is forward-looking, interactive and focused on practical solutions to real-world issues. If you are an information security practitioner or thought leader, we invite you to participate in this event by facilitating an educational session. Proposals are being accepted from those who are passionate about information security and willing to share their knowledge, expertise and experience. Join us at the Javits Convention Center in New York, NY USA, 20-21 November 2019. Be a part of this exciting collaboration of two global information security leaders.

PROPOSAL PROCESS
Phase 1: Speaker Proposals
Submit an abstract of your presentation topic clearly stating your methodology for audience engagement and identifying learning objectives and learning level. Please see the brief description of learning levels below and the full descriptions at the end of this document.

Beginner	Attendee has limited or no prior knowledge/experience with the subject matter. The session is intended to help attendees gain a working knowledge of the topic.
Intermediate	Attendee has a working knowledge of the topic covered but is not yet an advanced practitioner. The session is intended to help attendees build upon foundational knowledge and to advance understanding of the topic.
Advanced Technical	Attendee has a high level of technical understanding of the topic under discussion. The session is intended to contribute to the attendee's journey to mastery of a specific technical area.
Geek Street	Attendee has an extensive background in technology. These sessions are in-depth technical presentations and immersive, hands on experiences. The sessions should address the latest security risks and research into exploits, vulnerabilities and threats. Geek Street takes place on the expo floor rather than in the traditional session setting.
Advanced Managerial	Attendee has management experience and a high level of understanding of managerial concepts. The session is intended to contribute to the attendee's mastery of a specific managerial area or to build advanced leadership skills.

As part of your proposal, please indicate your presentation format (break-out session, panel, Geek Street as examples) and the length of your presentation. In addition to a 25-minute or 50-minute session, an option for a Master's Series is possible. Master's Series sessions are offered for an extended length of time (at least two hours). This allows in-depth coverage of a topic and more time for discussion.

Upon receipt of your proposal, we may contact you with questions for clarification or to gauge your interest in tailoring your proposal to meet a known need of our constituents.

Phase 2: Notifications
During this phase, you will receive notification whether your proposal has been accepted. If your proposal is not accepted, the basis may be that a large number of proposals were received in the same topic area or at your proposed learning level or format. Not receiving an acceptance should not deter you from submitting proposals for future conferences.

Phase 3: Presentations
Accepted proposals advance to the next phase, which is presentation preparation. Along with your acceptance notification, you will receive instructions for drafting your presentation. Once submitted, your presentation will be reviewed to ensure that the offering is at the appropriate learning level and that it fosters audience interaction. If there are questions or concerns regarding the content, we will collaborate with you. We do, however, reserve the right to require that changes be made.

Attendees have made it clear that having session presentations available *prior* to the event is a significant benefit and helps them get the most out of each session. To ensure that our attendees receive this benefit, **Infosecurity and ISACA ask that each speaker commits to submitting their final presentation to ISACA HQ on or before the deadline** *(to be established).*

MAKING YOUR PROPOSAL STAND OUT
- Engaging the audience
  Attendees expect more out of their conference education experience—more hands-on learning, more interaction with the presenter, and more opportunities to dive deeper into certain topic areas. We strongly encourage you to be creative and to thoroughly describe how you intend to deliver an interactive type of learning environment. Less presentation, more discussion.

- Tailoring your presentation to the audience
  Most attendees are IT professionals with 10+ years of experience in Security/Cybersecurity, Audit, Risk, Governance and Compliance. Given that, we strongly encourage you to submit a presentation at the Advanced Technical or Advanced Managerial learning level. If, however, you are proposing a presentation at either the Beginner or Intermediate learning level, an intriguing twist in a traditional area or a case study approach may increase the likelihood of acceptance. For advanced sessions, attendees may appreciate networking opportunities embedded in the learning experience: for beginner and intermediate sessions, however, attendees may prefer to focus more on real-world experiences.

- Aligning the learning objectives with the abstract
  Alignment between your proposal's abstract and learning objectives lays a solid foundation for the presentation. Also, during the proposal review process, clear evidence of this alignment gives us preliminary insight into how you plan to frame the session's presentation. Forward looking abstracts (i.e. future technology that is in development now) in tandem with learning objectives that are actionable are ideal.

BENEFITS OF SPEAKING AT INFOSECURITY/ISACA EXPO and CONFERENCE 2019

Speakers who are selected to present at the conference will receive the following benefits:

- Complimentary registration* for the conference – up to a $1,550 value! This includes the opportunity to earn up to **23 CPE** hours for conference participation *(complimentary registration is given to 1 speaker per session only)*
- Additional CPE hours for the session they present (*CPE hours for speakers are earned at <u>five times</u> the presentation time for the first presentation of the topic or an extensively modified topic*)

*Complimentary registration is not transferable or able to be used as a credit. Registration for the pre- and post-workshops are not included with complimentary conference registration.

Any speaker who receives an average score of 4.75 or higher on the session surveys will also receive special formal recognition from ISACA HQ and will be named as a **Top-Rated Speaker** on the ISACA conference web page at the conclusion of the conference. This score will be calculated from the average score of the questions on the mobile app session survey that are specifically related to the speaker and the presentation. At least 20 attendees must respond to the session's survey in order to qualify. Further, the top 5 rated speakers of the conference may be invited back to present at a future ISACA conference.

TRACKS FOR THE CONFERENCE
The list below highlights topics of interest for session proposals. Possible talking points are included for a few of the topics as examples.

If your proposal aligns with one of the tracks below, but is not specifically listed, simply submit it under the most appropriate track. Do you have an idea for a track that is not listed below that should be offered at this conference? We want to know! Submit your new track idea under the "New Ideas" category and tell us why you think it should be included.

Track 1: Emerging security tools & techniques
- **Artificial Intelligence:** (the Good, the Bad and the Hype)
- **Machine Learning:** (image recognition or natural language processing)
- **Endpoints can be managed: how about end users?** (behaviour analytics)
- **Strategies and tools to strengthen cybersecurity ecosystems**
- **Cloud Security**
- **Advances in authentication** (biometrics, hardware authentication)
- **Data flow monitoring**

Track 2: Cyber threat intelligence & technologies
- **Trends in Zero-day attacks**
- **Emerging trends on dark web activity**

- **Computer anti-forensics**
- **New and emerging malware types and trends**
- **Trending threats with mobile devices** (data leakage, obsolete devices, etc.)
- **What's Old is New Again** (anatomy of macro-based threats)
- **Cryptojacking**

Track 3: Cybersecurity leadership & development
- **Turning a challenge into an opportunity:** business value of security investments
- **Skills gap:** solution driven discussion with take-away actions
- **Vendor sprawl**
- **Automation:** what it can and cannot achieve
- **Succession planning:** not just for senior level positions
- **Clear the fog around AI:** compare/contrast AI, machine learning and deep learning
- **Cybersecurity leadership:** being an effective leader when your organization wants a hero

Track 4: Security risk & compliance
- **Developing a framework for security policies and procedures**
- **Effective communication of security policies**
- **Regulatory compliance:** governance, risk and compliance when no one wants to listen
- **IoT: security and privacy**
- **Security/privacy in disruptive environments:** (existing security tools' suitability for cloud)
- **Geopolitics and cybersecurity**
- **Corporate culture and cybersecurity:** from fluffy to critical information security component

Track 5: Data analytics enhancing cybersecurity
- **Real time threat analysis**
- **Malware detection**
- **APT detection**
- **Cloud security**
- **Intrusion detection in Everything IOT**
- **Network forensics**
- **Big data processing**

Exhibition Hall Geek Street
- **Blockchain** (algorithms and threats)
- **Robotic process innovation**
- **Zero trust networks**
- **Data mining and cybersecurity**
- **Single point of failure?** (master algorithms and machine learning)
- **Bug bounty programs:** (can security practitioners learn/adopt from this model)?
- **Deep learning: (**at the application level)

[Submit your proposal and become a speaker](#)

QUESTIONS?

Please review the **Speaker FAQs** for potential presenters for ISACA Conferences. You can also contact ISACA's Learning Solutions Department at any time at +1.847.660.5670, or simply **click here to submit a question.**