NESTet 2016
Nuclear Education & Training

Berlin, Germany

Cybersecurity: Moving Forward with Online Nuclear Education and Training

Dr. Jane LeClair

Founder

National Cybersecurity Institute

Washington, D.C.

Security is a Necessity

But…We Are a Connected World

- Technology has brought us convenience

Those With Malicious Intent

- Convenience has cost us security

What do Hackers Want?

DHS 16 Critical Infrastructures

- Chemical
- Communications
- Dams
- Emergency Services
- Financial Services
- Information Technology
- Transportation Systems
- Water/Wastewater Systems
- Commercial Facilities
- Critical Manufacturing
- Defense/Industrial Base
- Energy
- Food and Agriculture
- HealthCare/Public Health
- Nuclear Reactors/ Materials/Waste
- Government Facilities

Cybersecurity

- We need to ensure Cybersecurity

Physical Security

- We devote much effort to physical security

Warnings from the NSA

Admiral Rogers, Head of NSA:
'Nation states are spending a lot of time and effort to gain access to the US power grid and other critical infrastructure'

Growing Cyber Attacks

- The Islamic State group is now using the Internet to launch cybersecurity attacks at U.S. targets. (cyber)
- Caitlin Durkovich, Department of Homeland Security
- The startling April 2013 sniper assault that knocked out a Pacific Gas and Electric Co.'s Metcalf substation is looking like the work of an insider. (physical) (insider threat)
- In just a year, the number of cyber attacks using sophisticated concealment techniques tripled, to 90 percent…in excess of 500 unique evasive techniques that are now in malware….Mark Fabro, Lofty Perch

Growing Cyber Attacks

- The increasing threat from advanced cyberattack programs with sophisticated features to ***hide*** from cyberdefenses.
- The evasion techniques include timing features designed to keep attack software programs dormant when investigators are looking for them, and malware with auto-start features that can go into action without an incoming command… Mark Fabro, Lofty Perch

Vulnerability Assessments

- *"In our experience in conducting hundreds of vulnerability assessments in the private sector, in NO case have we ever found the operations network, the SCADA system, or energy management systems separated from the enterprise network. On average we see 11 direct connections between those networks…"*
  Sean McGurk, Director NCCIC, DHS . The Subcommittee on National Security, Homeland Defense, and Foreign Operations. May 25, 2011 hearing.

- As we talk about sharing information and resources, we must keep 'vulnerability sharing' in mind as well.

Motivation and Means

- *Typical hacking is profit- or revenge- driven, but something targeting industrial control systems has much more scarier motivation behind it…"* Kurt Stammberger, senior VP of Market Development at Norse Corporation

- *"One of the main challenges in protecting ICS/SCADA networks is the fact that these ystems were not necessarily designed with cybersecurity in mind – security solutions have been layered on in a piecemeal fashion after the networks were operationsl, leaving ample room for attackers to compromise their functionality*,,," Eric Byrnes of Tofino Security

Air Gap Myth & Spear Phishing Attacks

- *A watering hold attack can be used on a website of a vendor infecting the computers of top engineers when they go to download a product spec sheet. Spear phishing can be used to attack the general business network and understand the target*…then infiltrate the ICS. Targeted Attacks on ICS Surge. ThirdCertainty (2015)

- *The cyersecurity risk is growing as nuclear facilities become increasingly reliant on digital systems and make increasing use of commercial off-the-shelf software which offers considerable cost savings but increases vulnerability to hacking attacks."* Cybersecurity at Civil Nuclear Facilities: Understanding the Risks (2015)

And the Human Side…

- *By 2020, 25 million Baby Boomers who make up more than 40% of the US Labor Force will be exiting the workforce in large numbers and leaving many jobs to be filled. With their departure, the work characteristics that define the Baby Boomer generation—results driven, ambitious, idealistic, competitive, optimistic, and people oriented may be lost unless companies creatively develop strategies to simultaneously retain older workers and transition their knowledge to younger workers*….Kathleen Davis, Maintain a Skilled Workforce with Training and Technology. Energy Central (2013)

A People Problem

- Wired communication pathway between the digital network and the Internet
- Wireless communication pathway between the digital network and the Internet
- Connection (authorized and unauthorized) of portable digital media and computing devices to the digital network
- Physical access (authorized and unauthorized) to the digital network (insider threat)
- Hardware/software supply chain (equipment from a supplier)

Human Nature

- Humans Make Mistakes
- Human Performance Errors

Train and Educate

- Train *and* Educate to reduce incidents

NCI Recognizing the Need

- Introduction to Cybersecurity MOOC
- Cyber Training Course for Engineers
- Online Course Cybersecurity for Utilities
- Online Certificate Programs
- Online Bachelors and Masters in Cybersecurity
- Cybersecurity concentration in Nuclear program
- Precertification training

National Cybersecurity Institute

- Training
- Webinars
- Symposiums
- Journal
- Research

- Podcasts
- Testbooks
- Exhibits
- Blogs
- Speaker Series

Online MOOC

- Free MOOC
- '*An Introduction to Cybersecurity*'
- 10,000 Participants
- Basic concepts of CyberSecurity
- Evolving dynamics of CyberSecurity

Free Online Course

- Grant From the American Society for Engineering Education (ASEE)

- Free *Online* Cybersecurity training course for Engineering professionals

Center for Professional Development

- Developed New Online Course
- ‘Cybersecurity for Utilities’
- Online precertification exam training
- Flexible Non-Credit Certificate Program

Degree and Certificate Programs

- MS in Cybersecurity – 30 cr
- Graduate Certificate
  Cybersecurity Management – 16 cr
- Masters in Business Administration – 33-48 cr
  Concentration in Cybersecurity Management
- BS Cyber Ops – 120 cr
  Cyber Ops Core – 51 cr
- BS IT Cybersecurity Technology Concentration – 120 cr
- Undergraduate Certificate in CS
- BS Nuclear Engineering Technology – 124 cr
- BS NET – 124 cr

MS in Cybersecurity – 30 cr

- Digital Crime Prevention and Investigation
- Communication Security
- Ethics, Legal, and Compliance Issues in Cybersecurity
- Information Assurance
- IT Risk Analysis and Management
- Cyber Attacks and Defenses
- Advanced Networking
- Project Management
- Capstone Project in Cybersecurity

Graduate Certificate Cybersecurity Management – 16 cr

- Ethics, Legal, and Compliance Issues in Cybersecurity
- Information Assurance
- IT Risk Analysis and Management
- Security Management Awareness
- Capstone: Special Topics in Cybersecurity

Masters in Business Administration – 36-51 cr
Concentration in Cybersecurity Management

- Core requirements – 24 cr
- Foundation requirements – 0-15 cr
- Concentration – 9 cr
  - Ethics, Legal, and Compliance Issues in Cybersecurity
  - Information Assurance
  - IT Risk Analysis and Management

BS Cyber Ops – 120 cr
Cyber Ops Core – 51 cr

- C++ Programming
- Microprocessors
- Computer Architecture
- Operating Systems
- Advanced Networking
- Internetworking with TCP/IP
- Secure Mobile and Cloud Computing
- Reverse Engineering
- Fundamentals of Information Assurance

- Cyber Security Defense in Depth
- Cyber Attacks and Defenses
- Computer Forensics
- Governance, Legal, and Compliance
- Security Focused Risk Management
- Secure Software Development / Analysis
- Cryptography
- Cyber Operations Capstone Project

BS IT Cybersecurity Technology Concentration – 120 cr

Technology Component

- Object-Oriented Programming
- Computer Systems Architecture
- Operating Systems
- Data Communications and Networking
- Database Concepts
- Software Systems Analysis and Design
- Overview of Computer Security
- Project Management
- IT 495 Integrated Technology Assessment

Cybersecurity Technology Component

- Computer Forensics
- Cyber Attacks and Defenses
- Business Continuity
- Securing Mobile and Cloud Computing Environments
- Large-Scale Cybercrime and Terrorism

Undergraduate Certificate in CS

- Introduction to Cybersecurity
- Computer System Security Fundamentals
- Cybersecurity Defense in Depth
- Large Scale Cybercrime and Terrorism
- White Collar Crime
- Cybersecurity Investigations and Case Studies
  - Total: 16 credits

BS Nuclear Engineering Technology – 124 cr

- Minimum of 124 credits:
  - 60 in arts and sciences
  - 48 in the technology component (including 16 upper level)
  - 16 in free electives including information literacy

BS NET – 124 cr

- Minimum of 124 credits:
  - 60 in arts and sciences
  - 48 in the technology component (including 16 upper level)
  - 16 in free electives including information literacy
    - **NEW Concentration in Cybersecurity** – 15 cr
    - **CYS250 - Fundamentals of Information Assurance**
    - **CYS260 - Governance, Legal, and Compliance**
    - **CYS300 - Computer System Security Fundamentals**
    - **CYS345 - Cyber Security Defenses in Depth / Nuclear focus**
    - **CYS455 - Business Continuity**

Training

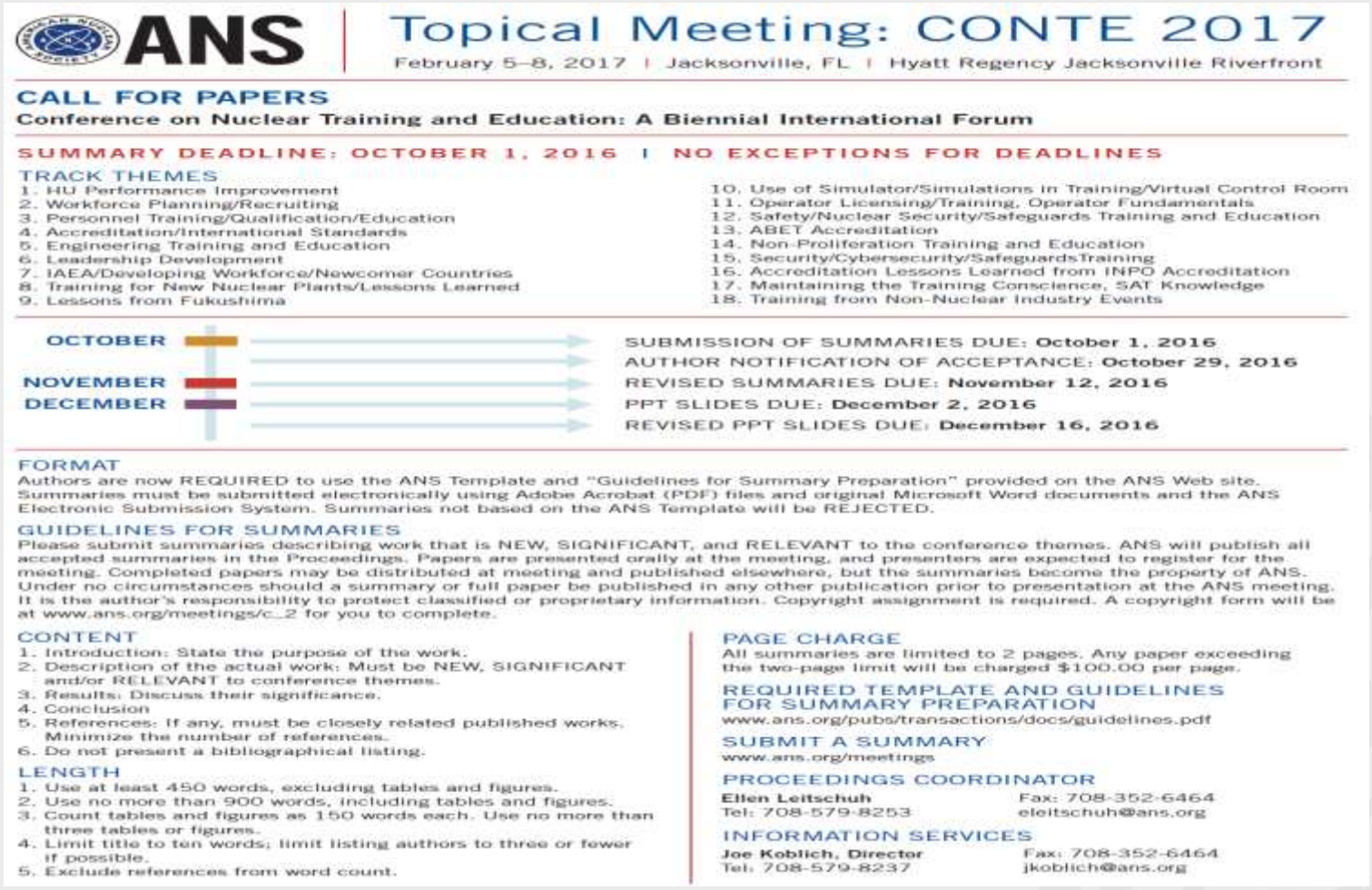
- CISSP
- HCISPP
- Security+
- CCISO
- Small Business
- Cyber Awareness
- C Suite & Board
- MOOC (10,000)

Improving Cybersecurity Culture

- *The Security CLTRe Toolkit uses social science principles and methodologies to measure ideas, customs and behaviors of employees. Finally, you can take the guesswork out of your security awareness activities, and start building a strong security culture to combat*

  cyberthreats! ….Kai Roer, CLTRe, https://get.clt.re/#/
- The Security Culture Conference 2016 is the leading global conference discussing how to build, measure and maintain security culture in organizations.
  http://securityculturereconference.com

CONTE 2017 – Feb 5-8, 2-17 Jacksonville, Florida



ANS | Topical Meeting: CONTE 2017

February 5–8, 2017 | Jacksonville, FL | Hyatt Regency Jacksonville Riverfront

CALL FOR PAPERS

Conference on Nuclear Training and Education: A Biennial International Forum

SUMMARY DEADLINE: OCTOBER 1, 2016 | NO EXCEPTIONS FOR DEADLINES

TRACK THEMES

1. HU Performance Improvement
2. Workforce Planning/Recruiting
3. Personnel Training/Qualification/Education
4. Accreditation/International Standards
5. Engineering Training and Education
6. Leadership Development
7. IAEA/Developing Workforce/Newcomer Countries
8. Training for New Nuclear Plants/Lessons Learned
9. Lessons from Fukushima
10. Use of Simulator/Simulations in Training/Virtual Control Room
11. Operator Licensing/Training, Operator Fundamentals
12. Safety/Nuclear Security/Safeguards Training and Education
13. ABET Accreditation
14. Non-Proliferation Training and Education
15. Security/Cybersecurity/SafeguardsTraining
16. Accreditation Lessons Learned from INPO Accreditation
17. Maintaining the Training Conscience, SAT Knowledge
18. Training from Non-Nuclear Industry Events

OCTOBER — SUBMISSION OF SUMMARIES DUE: **October 1, 2016**

AUTHOR NOTIFICATION OF ACCEPTANCE: **October 29, 2016**

NOVEMBER — REVISED SUMMARIES DUE: **November 12, 2016**

DECEMBER — PPT SLIDES DUE: **December 2, 2016**

REVISED PPT SLIDES DUE: **December 16, 2016**

FORMAT

Authors are now REQUIRED to use the ANS Template and "Guidelines for Summary Preparation" provided on the ANS Web site. Summaries must be submitted electronically using Adobe Acrobat (PDF) files and original Microsoft Word documents and the ANS Electronic Submission System. Summaries not based on the ANS Template will be REJECTED.

GUIDELINES FOR SUMMARIES

Please submit summaries describing work that is NEW, SIGNIFICANT, and RELEVANT to the conference themes. ANS will publish all accepted summaries in the Proceedings. Papers are presented orally at the meeting, and presenters are expected to register for the meeting. Completed papers may be distributed at meeting and published elsewhere, but the summaries become the property of ANS. Under no circumstances should a summary or full paper be published in any other publication prior to presentation at the ANS meeting. It is the author's responsibility to protect classified or proprietary information. Copyright assignment is required. A copyright form will be at www.ans.org/meetings/c_2 for you to complete.

CONTENT

1. Introduction: State the purpose of the work.
2. Description of the actual work: Must be NEW, SIGNIFICANT and/or RELEVANT to conference themes.
3. Results: Discuss their significance.
4. Conclusion
5. References: If any, must be closely related published works. Minimize the number of references.
6. Do not present a bibliographical listing.

LENGTH

1. Use at least 450 words, excluding tables and figures.
2. Use no more than 900 words, including tables and figures.
3. Count tables and figures as 150 words each. Use no more than three tables or figures.
4. Limit title to ten words; limit listing authors to three or fewer if possible.
5. Exclude references from word count.

PAGE CHARGE

All summaries are limited to 2 pages. Any paper exceeding the two-page limit will be charged $100.00 per page.

REQUIRED TEMPLATE AND GUIDELINES FOR SUMMARY PREPARATION

www.ans.org/pubs/transactions/docs/guidelines.pdf

SUBMIT A SUMMARY

www.ans.org/meetings

PROCEEDINGS COORDINATOR

Ellen Leitschuh
Tel: 708-579-8253
Fax: 708-352-6464
eleitschuh@ans.org

INFORMATION SERVICES

Joe Koblich, Director
Tel: 708-579-8237
Fax: 708-352-6464
jkoblich@ans.org

Cybersecurity

- A Key Strategy to Keep Our Nuclear Stations Secure

Final Thoughts…

- *Remember…..it's a rare event…when a senior leader comes to a board meeting and announces their company is NOT prepared for a cyber attack…..*
- *Average budget for cybersecurity is 1-5% of the annual budget*
- *YET 64 % of senior leaders surveyed feel they are not prepared or minimally cyber ready*
- *Leaders need to ask questions*

Summary

- Cyber attacks are growing
- Our data systems need to be protected
- Training and education is needed

Questions?

Dr. Jane LeClair

Founder

National Cybersecurity Institute

2000 M St. NW Suite 500

Washington, D.C.

www.NationalCybersecurityInstitute.org

jleclair@excelsior.edu