Cyber Security in the Nuclear Age

Dr. Jane LeClair,
Chief Operating Officer
National Cybersecurity Institute at Excelsior College
Washington, D.C.

NATIONAL CYBERSECURITY INSTITUTE AT EXCELSIOR COLLEGE®

Overview

A Vested Interest

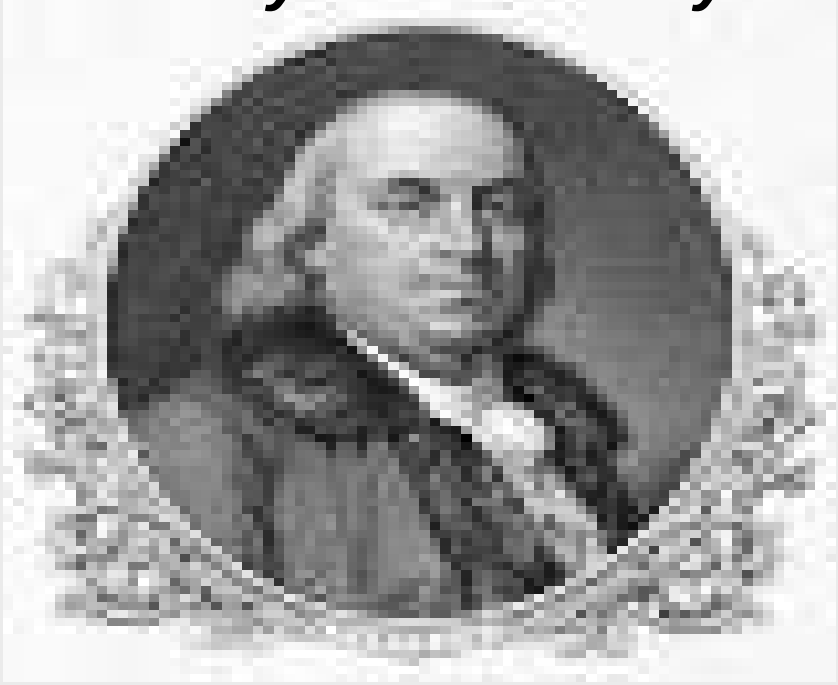
Computers have provided the means…

the Internet has provided the pathway

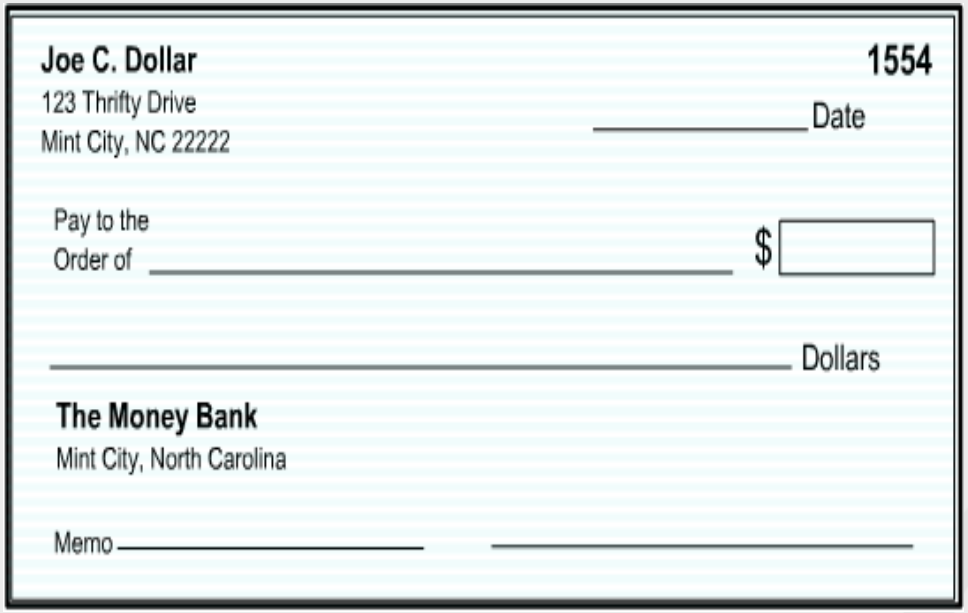
We are a Connected World

Security for Convenience

"If you sacrifice security for freedom you deserve neither"



Security for Convenience



Staggering Losses

Identity theft costs Americans $37 BILLION annually

Worldwide cyber crime costs about $1 TRILLION annually

Cybercrime cost US economy over $70 BILLION annually

Cybersecurity Timeline

Cybersecurity Timeline

Cybersecurity Timeline

Not ‘IF’- but ‘WHEN’

- In 2013…
  - Federal agents notified more than 3,000 U.S. companies last year that their computer systems had been hacked
  - White House officials revealed to industry executives how often it tipped off the private sector to cyber intrusions

Cyber Crime


P.F. CHANG'S


HomeGoods
Marshalls
T.J.maxx


LOCKHEED
MARTIN


MasterCard


TARGET


Neiman Marcus

What's It All About?

Wired Communication

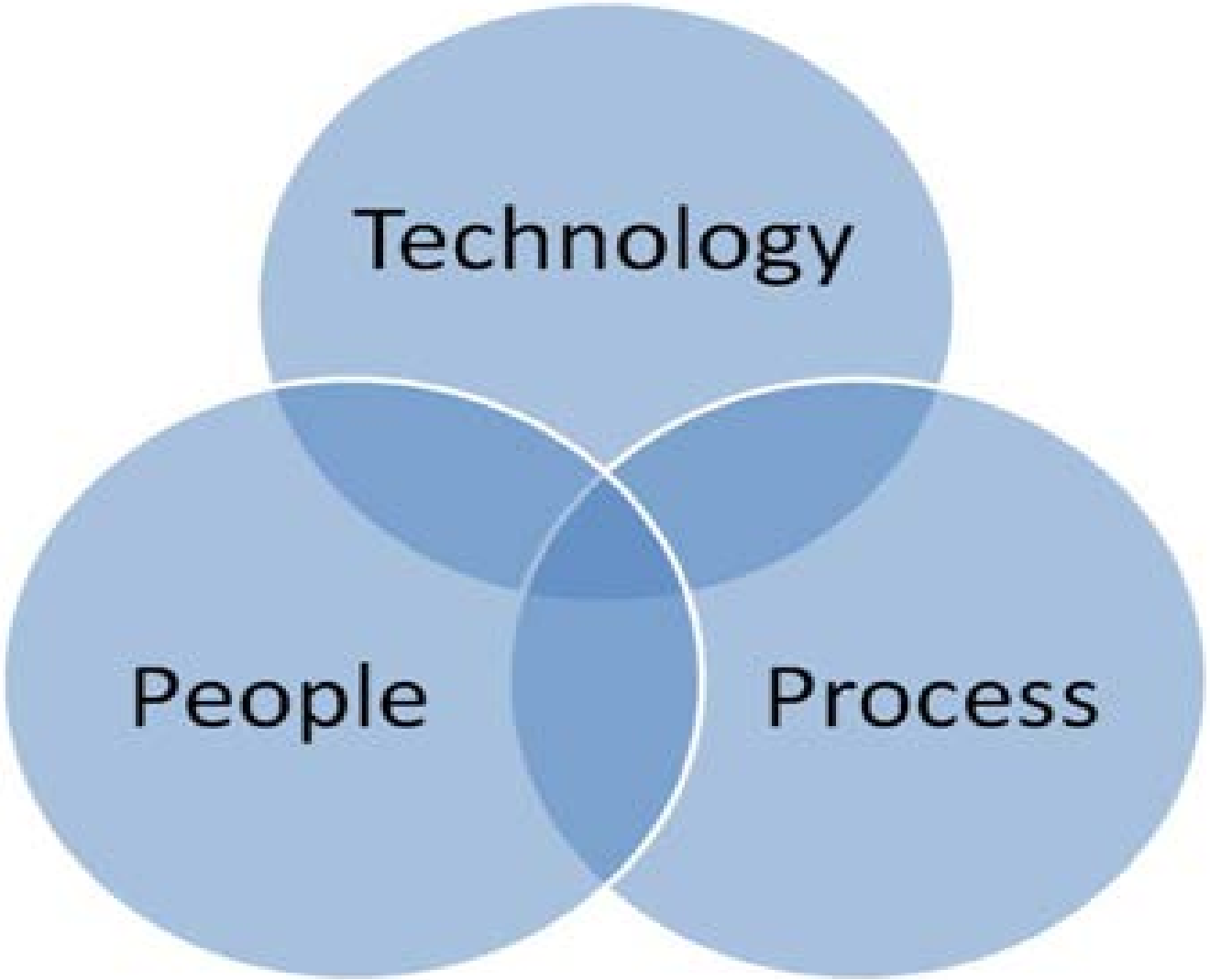
Wireless Communication

Connections

Supply Chain

Physical Access

Integrating the Domains



People Element

- Cyber security professional does not work on an island, but requires building bridges
- Human errors as major cause of security breaches
- Psychology/behavior/motives of hackers

Process Element

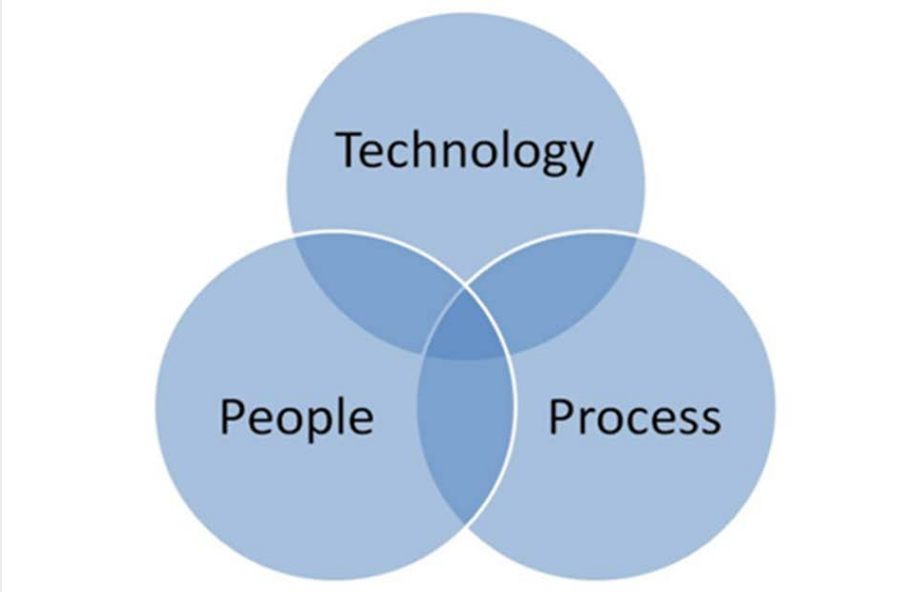
- Integrating solutions into existing procedures of organization
- Procedures must be well documented and established in organization
- Procedures must be revised on regular basis

Technology Element

- Basic understanding of core technical areas
- Programming, computer architecture, operating systems, database concepts, etc.

Integrating the Domains

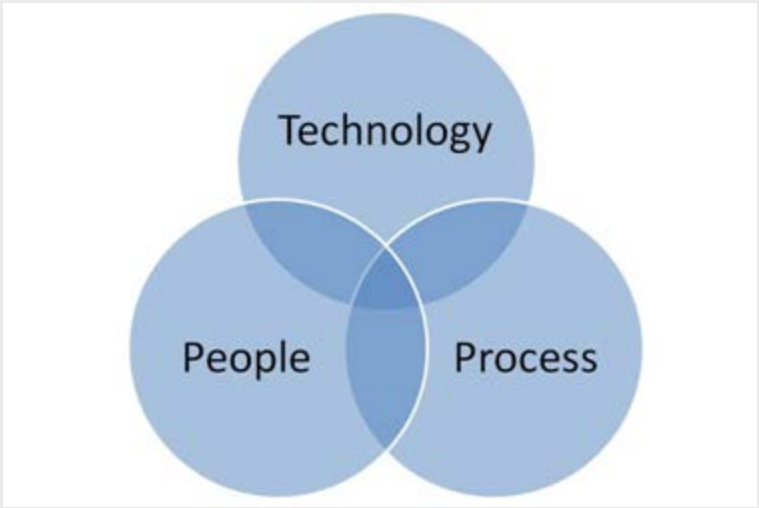
Education



Training

Framework for Cyber Security Online Education Integration

Integration



Supporting Online Learning Activities
•Discussions
•Group Projects
•Online Presentations
•Case Study Analysis
•Scenario Based Learning
•Interaction Activities
•Research Projects
•Collaborative team based learning
•Virtual Lab
•Team Virtual lab
•Online Cyber competitions

Integrating the Elements

Element	General Skills Desired	
PEOPLE	• Communication • Management • Collaboration	• Team Work • HCI (Human-computer Interaction) • Criminal Psychology
PROCESS	• Technical Writing • Project Management	• Critical Thinking • Team Work
TECHNOLOGY	• Programming • Computer Architecture • Operating Systems • Data Communications and Networking	• Database Concepts • Computer Security • Security tools • System Analysis and Design

National Institute of Standards and Technology (NIST)

Nuclear Information Technology Strategic Leadership (NITSL)

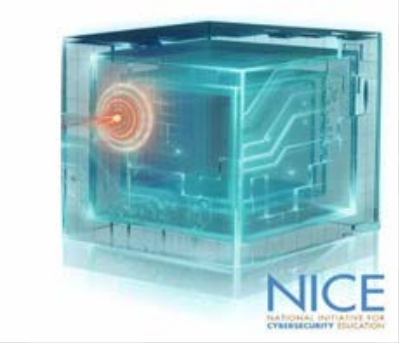
- NITSL is a nuclear industry group with membership from all utilities
- Members exchange pertinent information regarding evolving technologies issues
- Participants collaborate to address the many issues related to information technologies as utilized at nuclear facilities

Role of Cyber Security Education & Awareness

- As part of the Cyberspace Policy Review, President Obama identified cyber security education and awareness as a key gap.
- CE&A leads the following activities that are filling this gap:
  - Cyber Awareness Programs
  - Formal Cyber security Education
  - National Professionalization and Workforce Development Program
  - Training and Education Programs
  - Strategic Partnerships

National Initiative for Cybersecurity Education (NICE 2.0)

- NICE is a federally-endorsed program that interacts directly with academia and private industry on cyber security workforce issues.
  - NICE Component 1: Enhance Awareness
  - NICE Component 2: Expand the Pipeline
  - NICE Component 3: Evolve the Field



National Cybersecurity Workforce Framework

Defining the Cyber Workforce

- The US can benefit from greater consistency in classifying cyber security workers.
- Identifying and quantifying individuals performing cyber security work remains a challenge.
- Organizations realize the need to determine specific types of demand for cyber security workers.
- Government, private industry, and academia can create more effective cyber workforce structures by increasing collaboration and communication about the cyber workforce.

The National Centers of Academic Excellence in Information Assurance

Committee on National Security Systems

OLD

- Two-step process sponsored by **NSA**
  1. Committee on National Security Systems (CNSS) Training Standards as a prerequisite
  2. Recognition as a Center for Academic Excellence
     - CAE - Information Assurance Education
     - CAE - 2 Year Education
     - CAE - Research

NSA/DHS Information Assurance /Cyber Operations Designation

- Goal is to replace existing programs designated as CAE/IAE, CAE/2Y and CAE/R and **replace** the two step process CNSS/CAE
- Designation moves from Program to College level recognition
- Creation of a designation to distinguish strengths of each CAE Institution
- Benefit for students, employers, hiring managers throughout the nation
- New designation will be *NSA/DHS* CAE Cyber Operations and will replace previous designations

NEW

Criteria for Measurement CAE

1. Academic Content
2. Cyber Operations Recognized via Degree, Certificate or Focus Area
3. Program Accreditation or Curricula Review
4. Cyber Operations treated as an Inter-Disciplinary Science
5. Cyber Operations Academic Program is Robust and Active
6. Faculty Involvement in Cyber Operations-Related Research
7. Student Involvement in Cyber Operations-Related Research
8. Student Participation in Cyber Service-Learning Activities
9. Commitment to Participate in Summer Seminars Provided by the CAE-Cyber Operations program
10. Number of Faculty Involved in Cyber Operations Education and Research Activities

Criterion 1 Academic Content

- Program must include knowledge units covering
- 100% of the mandatory academic content
- 60% of the optional academic content

Criterion 1 Mandatory Academic Content

1. Low level programming languages
    - C programming, Assembly Language programming
2. Software reverse engineering
    - Reverse engineering for software specification recovery, malware analysis, tools, techniques, communications
3. Operating system theory
    - Privileged vs non-privileged states, Concurrency and synchronization, processes and threads, process/thread management, inter-process communications, Memory management/virtual memory, Uni-processor and multi-processor interface and support, File systems, IO issues, Distributed OS issues
4. Networking
    - Routing, network, and application protocols

Criterion 1 Mandatory Academic Content

5. Cellular and Mobile Communications
    - Smart phone technologies, Embedded operating systems, Mobile protocols, Infrastructures, Core network
6. Discrete Math
    - Algorithms, Statistics, Calculus I and II, Automata
7. Overview of Cyber Defense (must include hands-on lab)
    - Network security techniques and components, cryptography, Malicious activity detection
8. Security Fundamental Principles
    - Domain separation, Process isolation, resource encapsulation, Least privilege, Layering, Abstraction, Data hiding, Modularity, Simplicity of design, Minimization of implementation

Criterion 1 Mandatory Academic Content

- 9. Vulnerabilities
  - Vulnerability taxonomy, Root causes of Vulnerabilities, Mitigation strategies for classes of vulnerabilities
- 10. Legal
  - Laws, Regulations, Directives, Policies

Criterion 1 Optional Academic Content

1. Programmable logic languages
    - Hardware design languages, Hardware programming Languages
2. FPGA design
    - Synthesize, simulate and implement a programmable logic program
3. Wireless security
    - 2G, 3G, 4G, WiFi, Bluetooth, RFID
4. Virtualization
    - Virtualization techniques, Type 1 and Type 2 virtual machine architectures, Uses of virtualization for security, efficiency, simplicity, resource savings
5. Large scale distributed systems
    - Cloud computing, cloud security

Criterion 1 Optional Academic Content

6. Risk management of information systems
    - Models, Processes
7. Computer architecture
    - Logic design
8. Microcontroller design
    - Integrate discrete components
9. Software security analysis
    - Source code analysis, binary code analysis, Static code analysis techniques, Dynamic code analysis techniques, Testing methodologies
10. Secure software development
    - Secure programming principles and practices, Constructive techniques

Criterion 1 Optional Academic Content

11. Embedded systems
    - Program microcontrollers to achieve an application-specific design
12. Forensics and incident response or media exploitation
    - Operating system forensics, Media forensics, Network forensics, Component forensics
13. Systems programming
    - Kernel intervals, Device drivers, Multi-threading, Use of alternate processors
14. Applied cryptography
    - Use of symmetric and asymmetric encryption
15. SCADA systems
    - Embedded systems in industrial infrastructures and control systems

Criterion 1 Optional Academic Content

16. HCI/Usable Security
    - User interface issues
17. Offensive Cyber Operations
    - Phases of cyber operation
18. Hardware Reverse Engineering
    - Fundamental procedures such as probing, measuring and data collection to identify functionality and affect modifications

Criterion 2 Cyber Operations Recognized via Degree, Certificate or Focus Area

- Cyber Operations must be explicitly recognized as a focus area or specialization and students must meet requirements to be awarded such recognition

Criterion 3 Program Accreditation or Curricula Review

- Accreditation of the academic program (CS, EE, CE) on which the proposal is based will be considered a significant plus. All programs will undergo an in-person curriculum review

Criterion 4 Cyber Operations Treated as an Inter-Disciplinary Science

- Cyber operations concepts must be integrated into foundational curriculum courses as appropriate

Criterion 5 - Cyber Operations Academic Program is Robust and Active

- Evidence that courses are maintained current and offered frequently (e.g. every 18 months)

Criterion 6 Faculty Involvement in Cyber Operations-related Research

- Evidence of faculty grants, papers published, conference presentations related to the field of Cyber Operations

Criterion 7 Student Involvement in Cyber Operations-related Research

- Evidence of student work on grant research, papers published, conference presentations related to the field of Cyber Operations

Criterion 8 Student Participation in Cyber Service-Learning Activities

- Evidence of participation in local/ regional/ national cyber exercises, outreach to community colleges and high schools, etc.

Criterion 9 Commitment to Participate in Summer Seminars Provided by CAE-Cyber Operations Program

- First application: stated commitment
- Renewals: 2 students and 1 faculty member per year

Criterion 10 Number of Faculty Involved in Cyber Operations Education and Research Activities

- At least 2 faculty actively teaching cyber

Cyber Landscape

- Job Market
  - Dept of Labor expects 37% increase in cyber jobs 2018
  - Wall Street Journal expects cyber jobs to be 12 times the overall job market in near future
  - 50,000 vacancies in cyber positions in federal government alone
  - 22% vacancy in cyber positions in Department of Homeland Security
  - Cyber positions have $70-120k salaries with 101K as average
  - Biggest market is in DC, VA, and MD
  - Nationally there were 210,000 postings for cyber security positions in 2013

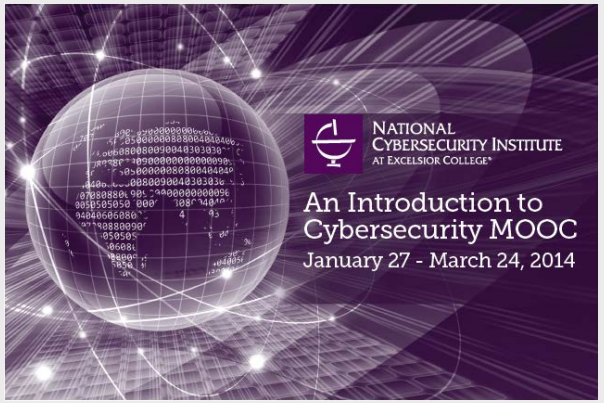
National Cybersecurity Institute's Role in Cyber

The National Cybersecurity Institute (NCI) was created for the purpose of conducting research, promoting educational and training opportunities within the cybersecurity field, and becoming a national resource for today's workforce.

National Cybersecurity Institute

Volume 1 & 2

MOOC JANUARY 2014 & SEPTEMBER 2014



CYBER TRAINING

Webinars

NCI Fellows

CISO Surveys

16 Critical Infrastructures

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

Cybersecurity and Government: Federal, State, and Local

- We entrust a great deal of information to the government at all levels
  - SS numbers
  - Health records
  - Income records
  - Personal data
- Government agencies are prime hacker targets

Cybersecurity and the Military

- The defense of our nation should be of prime concern to us all
  - Russian backed hacking groups (Energetic Bear) constantly seek to intrude on defense agencies
  - Chinese backed hacking groups (Deep Panda) constantly seek to intrude on defense agencies
  - Pentagon systems attacked *millions* of times per day
  - Defense contractors attacked

Cybersecurity and Health Care

- As the Affordable Care Act (*ObamaCare*) moves forward, more and more of our health records and personal information will be entrusted to government computer networks
- Modern medical procedures seek to share information among practitioners to benefit patient resulting in privacy issues
- Health Insurance Portability and Accountability Act - HIPPA – seeks to protect sensitive information

Cybersecurity and Telecommunications

- Regional disruptions of service highlight how much we depend on telephones
- Interwoven technologies with Internet and mobile devices
- Verizon hacked in 2013, AT&T hacked in April 2014

Cybersecurity and Finance

- What if Wall Street shut down?
  - Nasdaq breached in 2011 and digital bomb was uploaded
- Is your bank safe?
  - Banks are constantly under attack
  - Banks lose $11 billion annually in ATM fraud alone
  - American Bankers Association demands Congress act on hacking legislation

Cybersecurity and Utilities

- Is our electrical grid safe?
  - 2013 Shootout at Watts Bar
  - 2013 Sabotage at substation in CA
  - 2014 Russian backed hacker group ‘Dragonfly’ launched cyber attack on utility industry
- Threats
  - Wired and wireless communications
  - Insider threats
  - Supply Chain
  - Portable media

Cybersecurity in Education and Training

- There is a shortage of highly skilled cybersecurity professionals
  - The shortage is increasing
- We need to train and educate tens of thousands
  - Evolving skills and technology
  - Theoretical knowledge
  - Educate for the long term
  - Mentors and involve the underserved
  - Expand centers of academic excellence

Protecting our Future: Educating A Cybersecurity Workforce V2

- Cybersecurity and the Chemical Industry
- Cybersecurity and Commercial Facilities
- Cybersecurity and Critical Manufacturing
- Cybersecurity and Water and Dams
- Cybersecurity and Emergency Services
- Cybersecurity and Food and Agriculture
- Cybersecurity and Transportation
- Cybersecurity and Information Technology

Why We're Here

911

- Wake up Call
- Physical and cyber security
- Realization that assets had to be protected
- Call to Action for Nuclear industry
- Improved physical security
- Improved cyber security
- Implement /improve training and education on security/ cybersecurity

Five Attack/Threat Vectors

1. Wired communication pathway between the digital monitoring/control system and the Internet
    1. Supervisory Control and Data Acquisition (SCADA) network
2. Wireless communication pathway between the digital monitoring/control system and the Internet
3. Connection (authorized and unauthorized) of portable digital media and computing devices to the digital monitoring /control system
    1. Software updates and data downloads in digital monitoring and control networks are typically accomplished by connecting a portable storage device or laptop to the network via a USB port
4. Physical access (authorized and unauthorized) to the digital monitoring/control system
    1. Insider threat
5. Hardware/software supply chain
    - Equipment from a supplier here or overseas

Training and Education Actions

- Cyber security threats evolve and are ongoing
- Training and education must be ongoing
- Educate and train on the latest:
  - Cyber threats
  - Hardware/software
  - Social engineering
  - Procedures

NCR 10CFR 73.54/NEI 08-09

- The nuclear industry must meet stringent cyber security requirements based on the NRC's regulation 10CFR 73.54/NEI 08-09. Every nuclear plant must complete, within a specified time, a full cyber security assessment as it pertains to their Critical Digital Assets

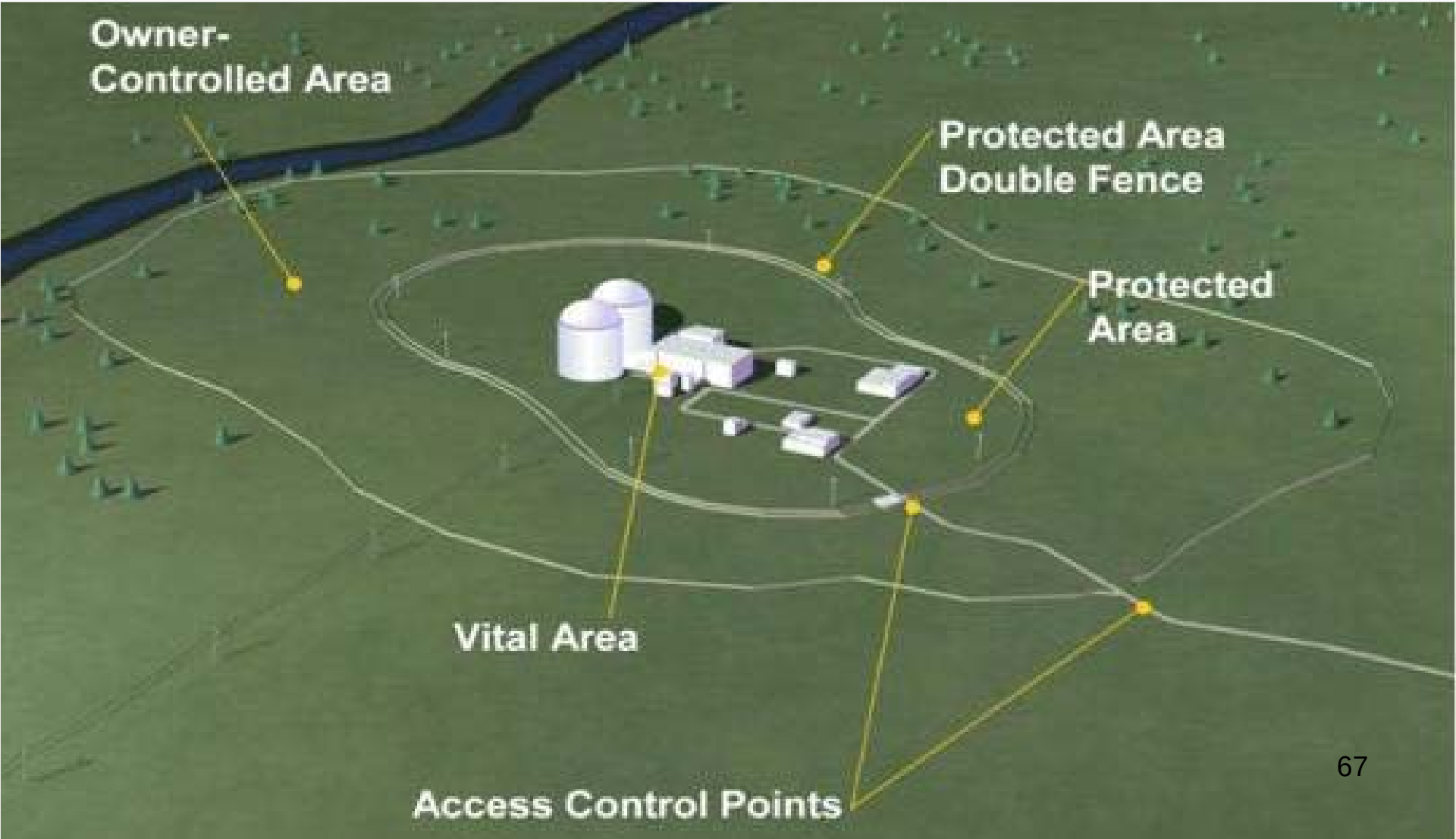
Milestones Established

- Establish cyber security assessment teams
- Identify critical systems and digital assets
- Level 3 / 4 isolation
- Regulate portable media and mobile devices
- Watchfulness for tampering
- Implement security controls for target set CDAs
- Ongoing monitoring of target set CDAs

Ongoing Workshops

Cybersecurity Standards

Physical Security



Data Security

Intrusion from the Outside

Security Measures

- Identification of the *power plant and grid systems and components* that are *critical* to safe and secure generation, transmission, and distribution of stable electric power to the nation.
- Identification of *digital monitoring and control systems* that are *critical* to the proper functioning of the above systems
- Implementing established *physical and digital protective measures* to *mitigate* wired, wireless, portable media and device, and physical *cyber-attack vector pathways* to the *critical* digital monitoring and control systems identified above; physical measures must include facility access authorization for personnel
- Developing and implementing *controls to mitigate* the cyber-attack vector pathway represented by *utility suppliers of hardware and software*

Security Measures

- Implementing methods and *programs to respond*, mitigate adverse effects, and recover from *successful cyber attacks*.
- Developing and implementing written cyber security *procedures* that utility company employees and contractors must follow, under penalties up to and including termination and prosecution
- Developing and implementing formal *work management processes* requiring workers to be certified for the work they perform and to have authorization from plant and grid operators to perform the work, on a specified schedule
- Developing and implementing *cyber security training* for utility company employees and contractors
- Implementing *programs* to continuously *monitor and mitigate* emerging *cyber security risks*

Intrusion From the Inside

Isolate ‘Protected’ Areas

Social Engineering

Where to go From Here

Today's Landscape

- Victims of our own success
- Emerging business opportunities expand the cyber attack surface
- We're not doing all we can
- Cyber threats defy conventional risk metrics

Preparation/Proactive Efforts

- Set the ‘Tone at the Top’ for organization
- Understand executive vulnerabilities
- Consider technical board members/committee
- Hire and validate right people and partners
- Detailed risk, resilience and plan review
- Exercise full plans across the enterprise
- Be unrelenting on oversight

Future Threats

- Ransomware
- Mobile – recent Apple vulnerability
- IOT – new sensors in old legacy systems
- Continued use of unsupported Windows XP
- Attacker information sharing

National Cybersecurity Institute

- √ Cyber Security Awareness
- √ C-Suite and Board Level
- √ Behavioral Awareness
- √ Insider threat
- √ Intelligence Awareness
- √ Medical Intelligence Awareness
- √ Cybersecurity Intelligence Awareness
- √ Vulnerability Assessment/Risk Management
- √ Cybersecurity Training for the Nuclear Industry
- √ Cybersecurity Training for the Health Care Industry
- √ Train-the-Cybersecurity Trainer

C-SUITE TRAINING

National Cybersecurity Institute

NATIONAL CYBERSECURITY INSTITUTE
AT EXCELSIOR COLLEGE®
www.excelsior.edu

National Cybersecurity Institute

IAEA
International Atomic Energy Agency

The Internship

American Nuclear Society

Excelsior College Cyber Programs

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 Conc – 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

Grad Certificate Cyber Mgmt – 16 cr

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

MS in Cybersecurity – 30 cr

- Digital Crime Prevention and Investigation (4 credits)
- Communication Security (4 credits)
- Ethics, Legal, and Compliance Issues in Cybersecurity (3 credits)
- Information Assurance (3 credits)
- IT Risk Analysis and Management (3 credits)
- Cyber Attacks and Defenses (3 credits)
- Advanced Networking (3 credits)
- Project Management (3 credits)
- Capstone Project in Cybersecurity (4 credits)

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

Cyber Concentration

Conclusions

Leadership must lead continuously

Growing threats, no easy fixes or panaceas

Shortage of talented defenders – choose wisely

People, partners, planning, & prevention critical

Continual learning and adapting required

Far bigger than just the IT organization

Questions

NATIONAL CYBERSECURITY INSTITUTE AT EXCELSIOR COLLEGE®

Contact Information

National Cybersecurity Institute
2000 M Street NW Suite 500
Washington, D.C. 20036
nci@excelsior.edu
jleclair@excelsior.edu
+1-202-601-1222