Securing Sensitive Information

Presentation at FCIX 2012
June 13, 2012

John Weidner
Corporate Security Director
USEC Inc.

Overview

- Success Stories:
  - NRC-Industry collaboration on NEI 08-11
  - Best Practices at USEC
  - Seoul 2012 – Securing Sensitive Information

- Credible threats and a path to success

NEI 08-11: Information Security Program Guidelines for Protection of Classified Material at Uranium Enrichment Facilities

- In 2007, NRC effort to issue Orders to enhance protection of classified enrichment technologies
- Enrichment plant licensees, in collaboration with NRC, developed voluntary guidance to meet the mutual goal of enhanced protection of classified information, equipment and technology.
  - "*Have we got a deal for you…the government will write your plan in this specific area*"
- Guidance has been modeled after programs mandatory for DOE contracts and programs, building on current NRC regulations
- Emphasis on employee awareness, risk assessments and technical security measures common in sensitive government security programs
- All program elements can be found in National Industrial Security Program Operating Manual (NISPOM)
- NRC endorsed industry document in July 2009
- Licensees have implemented guidance into their SPPP's

Best Practice at USEC

Three keys for preventing disclosure of classified information:

- Management attention
- Frequent awareness messages
- Expanded use of secure (classified) networks

Seoul 2012 Nuclear Industry Summit
Working Group 2 – Securing Sensitive Information

- Securing sensitive (nuclear) information referred to in Communique of the 2010 Washington Nuclear Summit
- CEO's and other senior management of ten companies form Working Group 2 (AREVA, CNNC, GEH, INB, JNFL, KEPCO, Sellafield, TENEX, URENCO, USEC)
- 2012 Summit overall aim:
  - to prevent non-state actors from obtaining the information or technology required to use nuclear material for malicious purposes, such as the making of nuclear weapons
- Nuclear industry further aim:
  - to protect its know-how from commercial espionage

Seoul 2012 Working Group 2 – Report Summary

- Best Practice and International Guidelines
  - IAEA documents, current and suggested
  - NEI 08-11
  - Sharing of best practice
  - Role for international non-governmental organizations
- Cyber Security
  - Recognition of recent attacks
  - Stuxnet malware prompts expanded government - industry dialogue
  - USEC cyber security workshop
  - NRC initiative with NEI and enrichers on counterintelligence program guidance
  - Countering the threat presented by the trusted insider
- Security Culture
  - IAEA guide, relatively new concept
  - Employee awareness of security threats
  - Precursors, questioning attitude and open environment

Seoul 2012 Working Group 2 – Recommendations

- Support the development of a common international guideline for management of sensitive nuclear information.
- Support the sharing of best practice on security of sensitive nuclear information.
- Continue to give attention to protecting against cyber threats.
- Further enhance the nuclear industry security culture.
- Apply a high standard of security measures to protect sensitive nuclear information, insofar as is reasonable and practicable.

2012 Seoul Summit Statements

- Joint Statement of the 2012 Seoul Nuclear Industry Summit
  - Enhance security culture by continuing to raise awareness among employees to the security threats and foster an open environment for reporting security concerns
  - Continue to focus on and strengthen security measures against increasing cyber threats
  - Approach security and safety in a coordinated manner, when pursuing nuclear safety or security
- Multinational Statement on Nuclear Information Security
  - Specific provision for training or other professional development activities for raising awareness and skills among senior security practitioners to reduce potential risk from the “insider threat”
  - IAEA’s guidance on Computer Security at Nuclear Facilities

“A credible threat exists…nuclear security is important”

- From IAEA Nuclear Series No.17, Technical Guidance, Computer Security at Nuclear Facilities, Reference Manual:

  “ A robust computer security culture is an essential component of any effective security plan. It is important for management to ensure that computer security awareness is fully integrated into the overall site security culture. The characteristics of nuclear security culture are the beliefs, attitudes, behaviour and management systems, the assembly of which lead to a more effective nuclear security programme. The foundation of nuclear security culture is recognition…that a credible threat exists and that nuclear security is important.”

A Credible Threat Exists – Trusted Insiders

- Klaus Emil Julius Fuchs
  - From late 1947 to May 1949, Fuchs gave his case officer the key data on U.S. production of U-235.
- Abdul Qadeer Khan
  - Convicted in 1983, in absentia, in a Dutch court for conducting nuclear espionage and sentenced to four years in prison.
- Roy Lynn Oakley
  - Sentenced in June 2009 to six years in prison for trying to sell parts of uranium enrichment equipment that he had stolen from a U.S. DOE facility.
  - *"…bringing to justice the trusted insider who would betray America for private gain.."*

A Credible Threat Exists – More Trusted Insiders

- Stuxnet

  Unnamed "architect" of plan to use spies and unwitting accomplices to introduce malware into Iranian centrifuge SCADA systems:

  "It turns out there is always an idiot around who doesn't think much about the thumb drive in their hand."

- "WikiLeaks"

  U.S. Army private accused of violating military computer security and leaking classified information:

  "Everyone just sat at their workstations…writing more stuff to CD/DVD. [The] culture fed opportunities…weak servers, weak logging, weak physical security, weak counterintelligence, inattentive signal analysis…a perfect storm."

- Flame

  Iran's Computer Emergency Response Team:

  'Flame' seemed designed to mine data from personal computers and was distributed through USB sticks rather than the Internet

Path to Future Successes

- "A credible threat exists"
  - Industry needs threat information to make risk informed decisions
  - Open source and Internet should be supplemented with timely threat bulletins and classified briefings
- "Nuclear security is important"
  - Many attributes of a positive safety culture apply to security culture
  - Some attributes of an effective security culture may seem at odds with safety culture – important item for management attention
- Government and Industry Collaboration
  - In some areas, the methods of protection have been prescribed
  - In other areas, determining risk will require government input
  - In most areas, more collaboration, *even government consultation*, will be needed to reach the mutually desired outcome of enhanced security