YOU CAN'T BE TOO CAREFUL

The Challenges of Cybersecurity in the Nuclear Industry

Every year, the number of computers in use is growing, creating more opportunities for cyberattacks. (Photo: istockphoto.com)

The number of computers people use and interact with is growing every year, creating more opportunities for cyberattacks. For example, contemporary automobiles contain no fewer than 12 digital input/output channels to control the engine, transmission, radio, antilock braking, keyless entry, anti-theft, telematics, etc. All of these potentially contain vulnerabilities susceptible to being 'hacked'.

Computer and information technology are evolving very quickly, at times outpacing our awareness of possible sources of cyber-vulnerabilities and ultimate attack. Additionally, cyberattacks are not limited to the workplace, but can also target the private lives of individuals.

One of the IAEA's main aims in improving cybersecurity is to enhance nuclear security culture, to change how people think, and change how they evaluate not just the adoption, but also the use, of technology.

"If nuclear professionals and their families are more aware of not just their physical space, but their digital space, they will be more cautious with regard to online information sharing and the use of technology. Information that seems innocuous can be combined with other information found elsewhere online and can prove to be very damaging. Google and similar Internet search engines are often the first tool hackers use in developing an attack plan," says Dudenhoeffer.

Project Officer for the National Coordinator for Counterterrorism and Security of the Netherlands, Ben Govers says, understanding of the threat is slowly permeating the nuclear industry. "The nuclear industry is facing the challenge of having to both broaden and deepen its existing defences in computer and information networks set against cyberthreats. The industry is—more or less—at the starting point of developing, implementing and expanding robust measures for protecting the information and control systems of nuclear facilities".

"The IAEA can play a leading role in this dynamic development," says Govers

Community of Helpers

The computer virus Red October was discovered in October 2012. It is estimated to have gathered sensitive information in more than 60 countries for up to five years while remaining undetected. Information gathered from infected networks could be reused in

future cyberattacks. This level of sophistication in cybercrime is becoming more and more common, and is another challenge with which nuclear security personnel must grapple.

The IAEA supports States at every level in their efforts to build robust and tested information and computer security programmes. The IAEA organizes regional training programmes; creates courses for professionals in nuclear security; publishes cybersecurity guidelines for nuclear facilities; and conducts regular international meetings where professionals can share expertise and have their most pressing questions answered by fellow practitioners and by IAEA experts.

The IAEA also incorporates information security assessments into the IAEA International Physical Protection Advisory Service (IPPAS).

IPPAS, a comprehensive review available to all countries with nuclear materials and facilities, advises States on more effective ways to protect their nuclear and radiological material.

Many organizations are working to address the growing cyberthreat. Partnerships in these areas are important. The IAEA has worked in conjunction with the International Criminal Police Organization— INTERPOL and the European Network and Information Security Agency (ENISA) in international exercises and in the development of cybersecurity guidance documents and training activities.

The @TOMIC 2012 international exercise on cybersecurity and nuclear security events including nuclear forensics is one example of the IAEA's involvement in international activities to increase cybersecurity awareness for protecting nuclear and other radioactive material assets. The exercise, sponsored by the Netherlands, involved 150 participants from 40 countries. The next exercise will be held in 2014: @TOMIC 2014.

"Because the IAEA has a respected position in the nuclear world, it can play a stimulating and leading role in the realization of guidelines or protocols, and in raising awareness about cybersecurity measures," says Govers, organizer of the @TOMIC events.

Same Old Threats

According to Dudenhoeffer, it's important Member States see the similarities between current threats, and the ones they faced 50 years ago.

The IAEA has introduced a number of programmes to educate States about these issues, and to help them manage the problem, and fight back.

"The threat actors remain the same. There have always been criminal elements attempting to steal from you or blackmail you. There have always been those who oppose you and your work—terrorists, or disgruntled employees. Nuclear and radiological facilities have always needed to be protected from these threats. The big difference now is that these threat actors can use computer systems on-site or remotely to do their dirty work," says the nuclear security expert.

Cyberthreats are an international challenge. The IAEA supports Member States in their efforts to build and test computer security measures to protect nuclear facilities.

(Photo: istockphoto.com)

Sasha Henriques, IAEA Division of Public Information.