

Impact of IoT (Internet of Things) on traditional Insider Threat Mitigation

Traditionally, nuclear Insider Threat programs have focused upon those individuals with trusted access to facilities and or sensitive information, the abuse of which could lead to unacceptable consequences. Prior to the advent of digital technology, “insider threat” was usually limited to physical attacks focused on theft or sabotage. Recent integration of remote connectivity, engineering support, integrated sensor networks and maintenance contracts have led to critical environments existing within and often dependent upon a complex web of constant communication. While this construct enables employees and trusted third parties to more effectively monitor and operate nuclear related processes, it also places a strain on traditional definitions of “Insider Threat” and requires consideration of both “Unwitting Insiders”, those whose actions enable a cyber attack without their intent, and “Unknowing Insiders” or cyber mules who’s compromised devices or accounts enable a malicious actor without their knowledge.

Against this backdrop of emerging insider challenges cyber programs have stepped up to address both the intentional cyber insider and the unknowing/unwitting participants. New programs educate the user on proper use of computers and applications, the threat of phishing emails and have implemented the use of mandatory kiosks to validate digital media prior to deployment in sensitive areas. This is all productive and worthwhile, but the new wave of Internet of Things, (IoT) creates even more nuanced cyber threats and a very real scenario in which the user themselves represent a walking digital asset and may not in fact even realize the potential that they create for abuse as a cyber insider.

This presentation looks at where insider threat mitigation is today, how the models differ from a person to person perspective vs within the computing world, especially that of critical systems automation, and where it will be in the near future as implanted medical devices, wearable technology and even Elon Musk’s “Neural link” become the norm and the ability to identify “Cyber Insiders” ceases to have any relevant meaning with regard to cyber threat mitigation.

Gender

Male

State

United States

Author: HOFFMAN, Rob (Idaho National lab, USA)

Presenter: HOFFMAN, Rob (Idaho National lab, USA)

Track Classification: CC: Information and computer security considerations for nuclear security