Chapter 57
SCIPS:
Using Experiential Learning to Raise Cyber Situational Awareness in Industrial Control System

Allan Cook
De Montfort University, UK

Richard Smith
De Montfort University, UK

Leandros Maglaras
De Montfort University, UK

Helge Janicke
De Montfort University, UK

ABSTRACT

The cyber threat to industrial control systems is an acknowledged security issue, but a qualified dataset to quantify the risk remains largely unavailable. Senior executives of facilities that operate these systems face competing requirements for investment budgets, but without an understanding of the nature of the threat, cyber security may not be a high priority. Education and awareness campaigns are established methods of raising the profile of security issues with stakeholders, but traditional techniques typically deliver generic messages to wide audiences, rather than tailoring the communications to those who understand the impact of organisational risks. This paper explores the use of experiential learning through serious games for senior executives, to develop mental models within which participants can frame the nature of the threat, thereby raising their cyber security awareness, and increasing their motivation to address the issue.

DOI: 10.4018/978-1-5225-5634-3.ch057

INTRODUCTION

The cyber threat to critical national infrastructure (CNI), underpinned by industrial control systems (ICS) is an acknowledged national security challenge (The White House, 2013). For several years, vulnerabilities have been reported in ICS, with observable increases in cyber threats between 2011 and 2015 (ICS-CERT, 2011, 2012, 2013, 2016). ICS often use operating systems, applications and procedures that may be considered unconventional by contemporary IT professionals. These systems have operational requirements including the management of processes that, if not executed in a predictable manner, may result in injury, loss of life, damage to the environment, as well as serious financial issues (Stouffer, Falco, & Scarfone, 2011; Lopez, Alcaraz, & Roman, 2013; Gao & Morris, 2014; Mitchell & Chen, 2014; Du¨bendorfer, Wagner, & Plattner, 2004). Several factors have contributed to the escalation of risks specific to control systems, including the adoption of standardised technologies with known security deficiencies, connectivity of control systems with other networks, the use of insecure remote connections, and widespread availability of technical information about control systems (ICS-CERT, 2016; GAO, 2004; Office, 2011; Wueest, 2014; Kaspersky, 2014).

Whilst the complexity of ICS may deter some opportunistic actors, capable antagonists, characterised as Advanced Persistent Threats (APTs), pose a credible risk (Center, 2013). In 2014, 55 percent of incidents investigated by ICS-CERT involved APTs or sophisticated actors (ICS-CERT, 2016). However, to date, there have been limited documented instances of such incidents (Langner, 2013; Bencsa´th, P´ek, Butty´an, & Felegyhazi, 2012). The North American Electric Reliability Corporation (NERC) characterised the possible frequency of these incidents as low, but with the capacity for significant impact (NERC, 2010).

Despite the infrequency of reported ICS incidents, the APT risk remains at large. By their nature, APT attacks are covert and difficult to detect, with a degree of tailoring available to the antagonist in order to achieve focused outcomes on the target network. However, it has been demonstrated that APTs follow a common attack lifecycle, performed in several phases, that can be broadly characterised as reconnaissance, preparation, execution, gaining access, information gathering and connection maintenance (Vukalovi´c & Delija, 2015). An analysis of advanced threat actors in 2013 detected 4,192 attacks associated with APT groups with 17,995 unique malware infections (FireEye, 2014). Therefore, an ill-prepared ICS operator may struggle to recover from an APT attack, as a well-trained response team that understands the nature of the antagonist is critical to success in APT incidents (Cole, 2012).

To address this potential threat, risk management literature asserts that a risk can be described as the answer to three questions; 1) what can happen? (i.e., what can go wrong?), 2) how likely is it that it will happen?, and 3) if it does happen, what are the consequences? (Kaplan & Garrick, 1981). However, as the level of incident reporting has not produced a sufficiently quantified and observable set of metrics for cyber attacks on ICS to inform generally-accepted risk models, there is limited value in the probability judgments based on such techniques (Cook, Smith, Maglaras, & Janicke, 2016a).

Raising awareness of a threat is an acknowledged risk safeguard, as it is argued that through knowing that there is the possibility of a hazard, in this case a cyber attack, it poses less risk than if we have no understanding of its potential impact (Kaplan & Garrick, 1981). Experts within the ICS field bring domain knowledge to bear to raise awareness, but it has been observed through experimentation that a calibration curve formed by subjective probability judgements is usually more extreme than the relative frequency of events (Merrick, Leclerc, Trenkov, & Olsen, 2015). This limits the credibility of the information provided by such experts, especially in light of the low frequency of recorded antagonistic