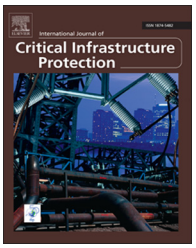
Available online at www.sciencedirect.com

ScienceDirect

www.elsevier.com/locate/ijcip



Evaluating the readiness of cyber first responders responsible for critical infrastructure protection

Jungsang Yoon[a], *Stephen Dunlap*[a], *Jonathan Butts*[b], *Mason Rice*[a,*], *Benjamin Ramsey*[a]

[a]*Department of Electrical and Computer Engineering, Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio 45433, USA*

[b]*QED Secure Solutions, 417 Forest Ridge Drive, Coppell, Texas 75019, USA*

ARTICLE INFO

Article history:
Received 11 January 2016
Received in revised form
12 February 2016
Accepted 15 February 2016
Available online 26 February 2016

Keywords:
Cyber attacks
Cyber emergency response personnel
Evaluation criteria
Training exercises

ABSTRACT

First responders go through rigorous training and evaluation to ensure that they are adequately prepared for emergencies. For example, fire departments continually evaluate the readiness of their firefighting personnel using a defined set of criteria that measures their performance in fire suppression and rescue procedures. However, in the cyber security domain, similar evaluation criteria and rigor are severely lacking for professionals who help detect, respond to and recover from cyber-based attacks against critical infrastructure assets. To address the gap, this paper provides a framework for evaluating the readiness of cyber first responders responsible for critical infrastructure protection. The evaluation criteria are conceptually based on the NFPA 1410 standards that are used to assess the readiness of firefighter first responders. The utility of the framework is illustrated using a military cyber training exercise that evaluated the readiness of professionals who respond to real-world cyber attack scenarios.

Published by Elsevier B.V.

1. Introduction

Evaluations of public safety first responders using realistic scenarios are vital to determining mission readiness. It is hard to imagine firefighters responding to emergency situations without proper assessments of their ability to perform firefighting tasks. It is inconceivable for a fire station to respond to a burning building without evaluating its personnel on the standard tactics required to fight fires. Indeed, it is critical that firefighters can perform tasks such as laying an initial attack line and back-up line, and obtaining the required water pressure within the time limit.

To evaluate the mission readiness of firefighters, fire departments often use the NFPA 1410 standards as a common set of criteria [2]. NFPA 1410 provides scenario-based standards that have been adopted by the community for evaluating the readiness of firefighter first responders. The standards use real-world scenarios and specify objectives, evaluation criteria and metrics for assessing firefighter readiness. The evaluation scenarios identify weaknesses in training regimens and provide assurance that personnel are ready to respond to emergencies in an appropriate manner.

Although common criteria guidelines have been used for decades to assess the readiness of firefighting personnel, this notion is in its infancy in the case of cyber professionals. Current evaluations rely primarily on exam-based certifications. However, this method of evaluation is woefully

*Corresponding author.
E-mail address: mason.rice@afit.edu (M. Rice).

http://dx.doi.org/10.1016/j.ijcip.2016.02.003
1874-5482/Published by Elsevier B.V.

inadequate given the responsibilities associated with critical infrastructure protection.

A cyber-based attack against a nation's critical infrastructure could have devastating consequences that would directly impact public safety. There is a growing awareness of the threats posed by cyber-based attacks and their implications, but little is being done to ensure the competence and preparedness of cyber professionals who are called upon to detect, respond to and recover from attacks.

To address the gaps, this paper presents a framework for developing common evaluation criteria for cyber first responders involved in critical infrastructure protection. The framework uses NFPA 1410 concepts to specify objectives, evaluation criteria and metrics for scenario development, and more importantly, response evaluation. The utility of the framework is demonstrated via a military cyber training exercise that applied NFPA 1410 concepts to evaluate cyber professionals and assess their ability to respond to realistic cyber attack scenarios.

2. Assessing readiness

It is imperative that first responders are continually evaluated against realistic scenarios. Firefighters undergo extensive training and evaluations that mirror real-world situations to ensure that they will respond adequately when called upon to perform their tasks. A common set of evaluation criteria helps prepare firefighters for such responses and helps identify training deficiencies that need attention. Unfortunately, similar criteria and rigor are severely lacking for cyber security professionals who respond to cyber-based attacks against critical infrastructure assets.

2.1. *Training standards for emergency scene operations*

Fire department personnel engaged in emergency scene operations use the NFPA 1410 Evolutions standards for training evaluation [13]. The standards specify criteria and metrics that can be adapted to local conditions and provide a strong mechanism for evaluating minimum acceptable performance during training activities.

Fig. 1 shows a representative evolution training standard for a handline-forward lead out operation. The example simulates a response to a typical building fire where a fire company must secure a hydrant and lay supply lines towards the building on fire. The firefighters are evaluated on their ability to correctly apply the forward lay water supply tactic to obtain the appropriate water pressure to suppress the fire.

The example highlights the various criteria used to evaluate a firefighting team and the maximum time to complete the objective. The NFPA 1410 standards provide numerous scenarios and criteria for evaluation that are based on tactics used in real-world incidents. It is important to note that the guidelines and criteria may be adapted to meet local as well as scenario-specific requirements.

2.2. *Cyber first responders*

Historical events have demonstrated the ability of cyber-based attacks to disrupt critical infrastructure operations [18]. Attacks against industrial control systems (ICSs) are on the rise and they increasingly target operations at power plants, factories and refineries [11]. The U.S. Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) has issued alerts for multiple campaigns (e.g., Havex RAT [4] and BlackEnergy [6]) that target critical systems by exploiting vulnerabilities in General Electric, Advantech/Broadwin and Siemens products [5]. A recent SANS report [20] claims that a cyber attack was responsible for a power outage in Ukraine in December 2015. According to the report, hackers likely compromised control systems and installed malware that tripped breakers, cut power and prevented technicians from detecting the attack.

Attacks targeting a national critical infrastructure can produce devastating consequences. Organizations spend considerable amounts of money to hire and train cyber security personnel to prevent, identify and mitigate attacks [15]. From a maturity standpoint, however, the ability to evaluate the readiness of cyber first responders is in its infancy. Training is disparate and the requisite skill sets are not standardized [16]. Much attention has been given to frameworks for system security and organizational risk (e.g., NIST Framework for Improving Critical Infrastructure Cybersecurity [14]). However, organizations do not have a standard methodology for evaluating if cyber first responders are adequately prepared to respond to incidents.

Current evaluations of industrial control system cyber security skill sets rely primarily on professional certifications. The International Society of Automation (ISA) [8], a professional association, has developed a knowledge-based certificate program designed to test the security standards described in the ISA99 standard through a multiple choice exam. ISA99 provides guidelines in areas such as industrial control system security management, security risk assessment and system design, and technical security of industrial control system components. Similarly, the Global Information Assurance Certification [3] offers the Global Industrial Cyber Security Professional (GICSP) certification that tests industrial control system security professionals in essential knowledge areas such as access management, cyber security for industrial control systems, industrial control system architectures, industrial control system module and element hardening, and industrial control system security monitoring. The Information Assurance Certification Review Board [7] awards the Certified SCADA Security Architect (CSSA) certification to individuals who pass a 100-question exam on knowledge related to securing SCADA systems.

The primary concerns with certification programs are the lack of evaluation criteria against a common set of standards and assessments of the ability to apply knowledge, concepts and experience to real-time situations associated with actual exploitations of industrial control systems [10]. A European Union Agency for Network and Information Security (ENISA) study [16] that examined industrial control system certification programs recommends the development of a framework