Computers in Human Behavior 48 (2015) 51–61

Contents lists available at ScienceDirect

Computers in Human Behavior

journal homepage: www.elsevier.com/locate/comphumbeh

Effects of cyber security knowledge on attack detection

Noam Ben-Asher *, Cleotilde Gonzalez

Dynamic Decision Making Laboratory, Department of Social and Decision Sciences, Carnegie Mellon University, PA, USA

ARTICLE INFO

Article history:

Keywords:
Cyber security
Knowledge
Dynamic decision-making
Intrusion-detection system
Expertise

ABSTRACT

Ensuring cyber security is a complex task that relies on domain knowledge and requires cognitive abilities to determine possible threats from large amounts of network data. This study investigates how knowledge in network operations and information security influence the detection of intrusions in a simple network. We developed a simplified Intrusion Detection System (IDS), which allows us to examine how individuals with or without knowledge in cyber security detect malicious events and declare an attack based on a sequence of network events. Our results indicate that more knowledge in cyber security facilitated the correct detection of malicious events and decreased the false classification of benign events as malicious. However, knowledge had less contribution when judging whether a sequence of events representing a cyber-attack. While knowledge of cyber security helps in the detection of malicious events, situated knowledge regarding a specific network at hand is needed to make accurate detection decisions. Responses from participants that have knowledge in cyber security indicated that they were able to distinguish between different types of cyber-attacks, whereas novice participants were not sensitive to the attack types. We explain how these findings relate to cognitive processes and we discuss their implications for improving cyber security.

1. Introduction

Cyber-attacks—the disruption of computers' normal functioning and the loss of sensitive information through malicious network events—are becoming more widespread. Guarding against them is a significant part of the Information Technology (IT) governance done by cyber analysts, as many government agencies and private companies have moved to distributed systems (McHugh, 2001). The most important responsibility of a cyber-security analyst is to protect a network from harm. Many technological advances in information and network security have facilitated the advanced monitoring and threat detection for the analysts, but the tasks they perform cannot be completely automated. The analytical capabilities of the human decision maker are still needed and are indispensable (Cranor, 2008; Jajodia, Liu, Swarup, & Wang, 2010). However, although analysts are capable of performing cyber security tasks, our understanding of the cognitive processes that are required for effective network protection is relatively limited (Chen, Liu, Yen, & Mullen, 2012; Gonzalez, Ben-Asher, Oltramari, & Lebiere, 2014). Furthermore, it is unclear in what ways the analysts utilize their experience in cyber security to detect cyber-attacks.

One tool that security analysts heavily rely on is Intrusion Detection System (IDS). This tool can detect network intrusions and network misuse by matching patterns of known attacks against ongoing network activity. Once the IDS finds a match to a known type of attack or detects abnormal network activity, it produces alerts detailing the suspicious events (Goodall, Lutters, & Komlodi, 2009). In IDS, as in other alert systems, decreasing the number of missed events increases the number of false alerts (Green & Swets, 1966). Considering the amount of traffic in a mid-size corporate network and the ever-growing number and complexity of cyber-attacks, the number of alerts generated by an IDS can be overwhelming to a human analyst. Such systems can trigger thousands of alerts per day, up to 99% of which are false alerts (Goodall, Lutters, & Komlodi, 2004). Eventually, the high volume of intrusion alerts that needs to be processed and the high probability of false alerts make the process of accurately detecting a cyber-attack challenging for human cognitive capabilities.

There is a growing body of work within the cyber security field that is focused on understanding the work processes of security analysts (D'Amico et al., 2005; Goodall et al., 2009; Thompson, Rantanen, & Yurcik, 2006; Werlinger, Muldner, Hawkey, & Beznosov, 2010). Previous studies infer that the general cyber analysis work process model includes preparation, monitoring,

* Corresponding author at: Dynamic Decision Making Laboratory, Department of Social and Decision Sciences, Carnegie Mellon University, 4609 Winthrop Street, Pittsburgh, PA 15213, USA. Tel.: +1 412 268 9547.

E-mail addresses: noamba@cmu.edu (N. Ben-Asher), coty@cmu.edu (C. Gonzalez).

http://dx.doi.org/10.1016/j.chb.2015.01.039
0747-5632/

detection, analysis, and response to network events. Both monitoring and detection belong to a general process called *triage analysis*. When conducting triage analysis, the analyst screens a large number of IDS alerts and network events, identifies false alerts, and escalates suspicious events for further analysis, which can result in the appropriate response (D'Amico et al., 2005). Triage analysis is a knowledge-intensive activity in which an analyst's expertise is leveraged to promptly dismiss false alerts and to attend to alerts that provide true indications of a cyber-attack.

In this study, we investigate the basic cognitive processes involved in the detection of cyber-attacks with a specific interest in understanding the interplay between domain knowledge and cognitive skills. As one cannot play chess without knowing the rules of the game, some specific knowledge is required to detect cyber-attacks. Cyber security analysts and practitioners are required to have a broad knowledge of network operation and information security. They usually undergo extensive training and certification programs. However, it is not clear whether acquiring deep and detailed knowledge in cyber security is the main determinant of performance when detecting cyber-attacks or whatever the ability to efficiently apply general thinking strategies is at least equally crucial to this task. Furthermore, it is still unclear how aspects like information search and evidence accumulation, which serve as a basis for the detection of cyber-attacks, depend on the analyst's domain knowledge and on a general set of cognitive skills she apply (Perkins & Salomon, 1989). As the security analyst operates in a highly dynamic environment, domain knowledge can be incomplete or become outdated relatively fast. This type of environment highlights the dependability on thinking strategies for problem solving, inventive thinking, decision making, and learning. Thus, it is possible that mastering independent cognitive skills in such a context is a main component of cyber security expertise.

As an initial step in resolving these questions, we examine how the knowledge gap between experts and novices in cyber security influences their ability to detect cyber-attacks. A questionnaire allowed us to corroborate participants' knowledge in information and network security. Using a simplified IDS tool, we then conduct laboratory and online experiments with experienced individuals in cyber security and with participants with no significant knowledge of cyber security. We examined the intrusion detection process in different contexts (i.e., network scenarios) by presenting several types of cyber-attacks. For each network scenario, the intrusion detection process had two parts: the first included classification of network events as malicious or benign; and in the second part, a decision was made about whether or not the whole sequence of network events represents an ongoing cyber-attack. This allowed us to further examine the role of experience in different stages of the detection task. Overall, we predicted that a larger knowledge base would lead to better performance, and that experts would do better than novices that can only rely on their general cognitive skills. Therefore, we hypothesized that experts will be more accurate than novices, when judging a whole sequence of network events, and detecting a cyber-attack. We also expect that experts will decide more accurately whether a network event is malicious or not. Finally, we hypothesized that when judging a sequence of network events experts will be more confident in their decisions compared to novice. These differences, between experts and novices, are expected to be consistent across different network scenarios.

2. Knowledge and cognitive challenges of cyber security

The rate and the extent to which the cyberspace can change is extremely variable and unpredictable compared to other environments that are bound by physical constraints. The topology of the network, the services it provides, and the users who depend on these services are constantly changing. In parallel, new vulnerabilities that can be exploited continuously emerge, clever attack strategies are constantly developed and new counteracting protective measures are deployed. These challenges result in a continuous effort by the cyber security analyst to stay up-to-date on the knowledge needed to successfully defend a network.

An analyst continually monitors the network, identifies threats, and repairs each and any vulnerability; while the attacker only needs to find a single vulnerability that can be exploited (Yurcik, Barlow, & Rosendale, 2003). This simplified view highlights the asymmetric relationships between a security analyst, a complex environment, and an attacker. An analyst is constantly required to make multiple and interdependent decisions in a dynamic environment. Dynamic decision making is highly complex because it requires an understanding of multiple, interrelated attributes and the ability to anticipate the way that the environment will develop over time. A decision maker is also required to act at the right time to maximize the decision value (Brehmer, 1992; Edwards, 1962; Gonzalez, 2005; Gonzalez, Vanyukov, & Martin, 2005). Given the frequent and forcible changes in the cyber environment, an analyst has to make real-time decisions depending on past experiences and current knowledge.

Following Chi's (2006) view on the characteristics of expertise and the *relative* view of expertise (Chase & Simon, 1973), a cyber security analyst may be regarded as an expert with high levels of proficiency in information and network security when compared to a novice who is less knowledgeable. The term novice is used here in a generic manner, referring to a wide spectrum of individuals with relatively no knowledge of cyber security. The term "novices" also suggests that with proper training and with enough experience, individuals can become experts. More specifically, the relative view of expertise postulates that an expert is not expert due to some innate talent or cognitive ability that the novice cannot possess. Rather, a novice can become an expert with proper training. However, it is possible that some aspects of expertise depend on the ability to tune general cognitive skills, like sustained attention and information synthesis, to a specific context, providing contextualized ways to access and deploy domain specific knowledge (Perkins & Salomon, 1989).

Asgharpour, Liu, and Camp (2007) showed how individuals with various levels of knowledge in information security and years of experience, may have different mental models of cyber security. Higher proficiency in information security also suggests better performance in cyber detection than lower levels of knowledge. Experienced individuals are expected to make better decisions than inexperienced ones. An expert is expected to detect features and meaningful patterns that a novice cannot (Shanteau, 1987). Knowledge and previous experience should make an expert more sensitive to cues that are overlooked by a novice. Careful attention to these cues can foster the identification of patterns that construct a problem and should promote the choice of the appropriate courses of action. Such expertise appears to be domain specific, and it is built up through experience and intensive practice (Randel, Pugh, & Reed, 1996). However, expertise may be domain limited and context dependent. Expertise can also make individuals more rigid and result in problematic adaptation in more dynamic environments (Chi, 2006). Furthermore, depending only on domain knowledge and neglecting general cognitive skills and heuristics can harm the ability of experts to mitigate atypical problems.

Goodall et al. (2009) studied cyber security analysts and the practical aspects of intrusion detection. Their work particularly highlights the expertise required to successfully accomplish the intrusion detection task. It comprises of domain knowledge in information and network security, and also local knowledge