feature

Application of Situation Awareness in Incident Response

With the exponential increase in security incidents due to known and unknown causes, the responsibilities of the computer security incident response (CSIR) team have become more complex. Effective and efficient incident handling is required to stay abreast of these pervasive security incidents and a mature incident response (IR) process can be useful. To establish a mature and effective IR process, organizations should focus not only on the technical aspect, but also on human behavior through the situation awareness (SA) theory.

In a study to evaluate information security practices, it was revealed that the majority of security incidents are indirectly caused by insiders not following the security policies and lacking SA.[1] SA has been defined as "the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future."[2]

Organizations have typically built their detection and IR capabilities based on the available technology components without paying sufficient attention to the people or process dimensions of the solutions. Perhaps the environment, qualifications and skill levels acquired over time can influence the expected delivery of security objectives. IR personnel make decisions intrinsically based on security solutions coupled with good individual security practices; however, bad decisions can have enormous implications if SA is missing.

Teju Oyewole, CISA, CISM, CRISC, COBIT® Assessor, CISSP, CSOE, ISO 27001 LA, ITIL, MBCS, PMP
Has more than 16 years of experience providing IT services and solutions within various sectors, including insurance, finance, banking, telecom and retail. Currently, he works as a security/compliance specialist at Indigo Books and Music. Prior to this, Oyewole worked with British Telecoms, Sun Microsystems, Oracle UK Inc. and Citigroup, all in the United Kingdom. He possesses international experience across Europe, Africa and North America, demonstrating expertise to ensure regulatory compliance, conducting security reviews, developing security strategy, evaluating risk, and developing security policies and processes in accordance with applicable standards. Oyewole is currently pursuing a doctoral degree in cybersecurity at Capital Technology University (Laurel, Maryland USA).

This article focuses on the application of SA theory to the advancement of IR processes. The SA theory is analyzed in the following section, and insight on how best to apply this to IR improvements is also discussed.

Situation Awareness Theory

Human interactions in all facets of tasks have been the bedrock of performance, even in the most automated environment.[3] The human factors in the operations of many mission- and safety-critical environments such as aircraft, military and industrial controls are so crucial that SA is used to evaluate the operator's timely decision making.

The analysis of SA can be explained further by referencing the key words in the definition. Consider an aircraft as an entity or element within an airspace environment and the following:

- **Perception**—This occurs when a situation or hazard is perceived. A typical example is an event, such as the Iceland volcano that occurred in 2010,[4] identified by an air traffic controller or meteorologist.
- **Comprehension**—This follows the perception of the hazard and consists of understanding the significant meaning of the event, a key ingredient in making an informed decision. A typical example is when an air traffic command and control center directs an airliner around bad weather to ensure safety.
- **Projection**—The knowledge acquired in the perception and comprehension stages is the main input into forming a future action for the element under review. A typical example in this scenario is the ability an aircraft command and control center to know the right course of action due to previous weather patterns.

SA analysis is further illustrated in **figure 1**, which depicts the integration of the key components as mentioned and other factors in decision making.

The three integrated components of SA (red arrows) play a significant role in decision-making processes. The scope of SA analysis for the purpose

of this article is limited to these three integrated components. However, there are other factors that can affect the decision at any point in time. Goals and objectives, preconceptions, abilities, experience, training, system capability, interface design, stress and workload, complexity, automation, and information processing mechanisms (long-term memory and automaticity) are all components of both individual and environmental factors (green arrows). The resultant application of the human factors in advancing IR capabilities is discussed in this article.

IR Concept and SA Application

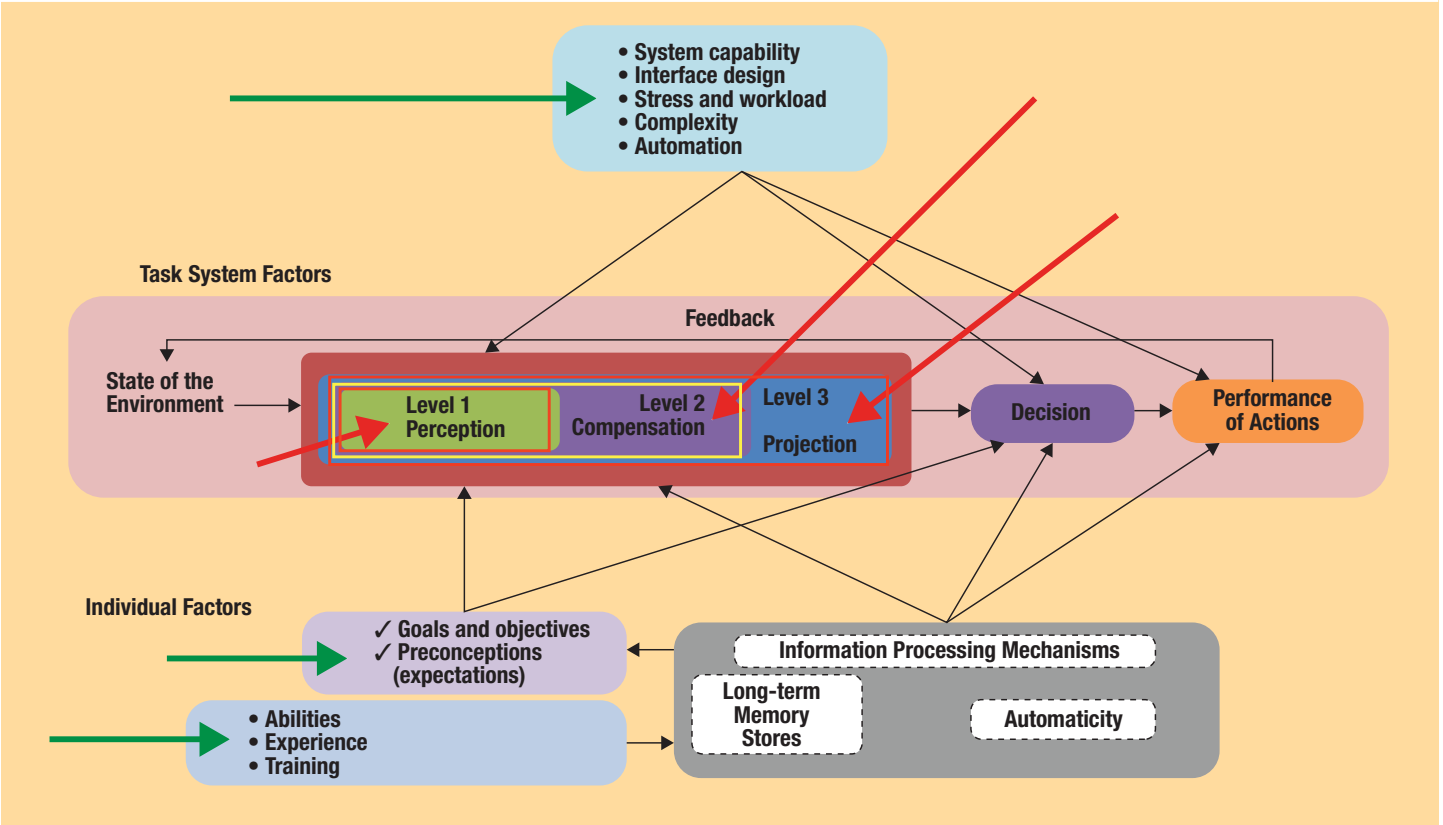
At the instance of incident response process illustrated in **figure 2**, the application of SA will be reviewed on key phases:

- Detection
- Analysis
- Containment
- Improvement

IR Detection

In this phase, incidents and events such as a change in the file or directory structure, failed logins, or dangerous executable codes are detected. This is accomplished primarily in real time by the automated security tools, but some can also be reported by users when unusual activities around systems are noticed.[5] Thus, critical response requires the right people with the right skills at just the right time in the right location.

Figure 1—Situation Awareness Model



Source: M. R. Endsley. Reprinted with permission

SA Application to IR Detection

During the detection phase of the IR, the very strong perception of hazard is necessary to foster effective and efficient decisions on how to proceed with the other phases. For example, an IR team member who possesses technical expertise, but lacks the common sense to interpret the detection can jeopardize the enterprise's security posture. The ability to identify the perceived hazard is a key component in SA. This kind of ability can be developed through repetitive actions or experiences. In fact, this leads to what is known as information security self-efficacy,[6] meaning the more individuals practice any task, the more robust their SA level becomes. Information security self-efficacy is an individual behavior that is combined with security tools for detecting events such as malware, sensitive data exfiltration and irregular login trials.

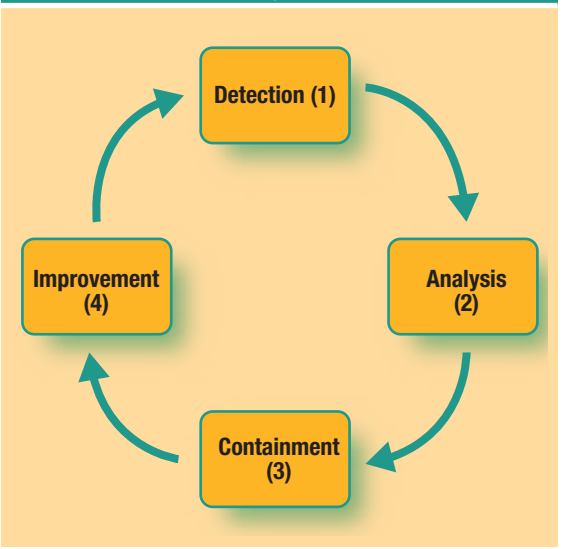
IR Analysis and Containment

Analysis of the detected incidents or events in the previous phase is where the actual consequences can be determined. The evaluation tasks are carried out through either manual or analytical tools and the next line of action—such as keep close monitoring, ignore or needs immediate action—is decided upon. In case of the latter action, the best effort may require containment in order to minimize the impact of the incidents or for the purpose of forensic evidence. IR personnel will apply due care as they deem fit according to the acquired SA.

SA Application to IR Analysis and Containment

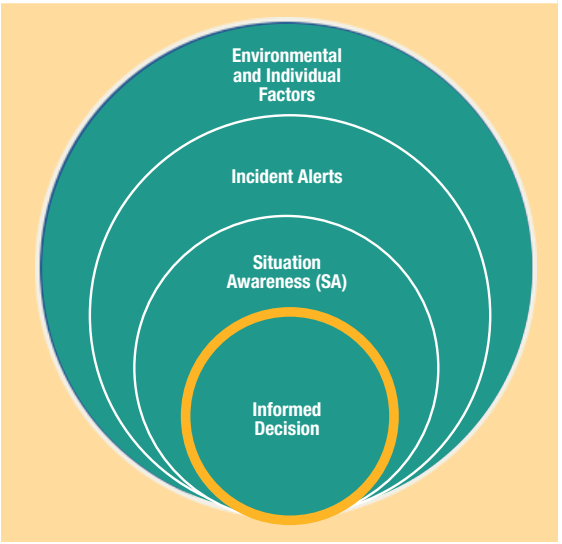
Understanding the consequential meaning of any incident requires coordinated efforts through the comprehension phase by the IR personnel. Comprehension at this level is of high importance for decision making. Though much of this analysis might have taken place within the security tools, there may be a chance of new and unknown security incidents and events such as those noticed or reported by users.[7] Analysis of new or multiple events can help contain the resultant malicious incidents in a timely manner. These are the phases where the IR personnel apply well-structured and fully comprehended information gathered from the detection phase in conjunction with any new, additional information at this phase.[8] These response efforts may require several tasks such as diplomacy, ability to work under pressure, problem-solving skills, curiosity, passion, adaptability, clear thinking and communication with other parties in order to gain more details about the incident that is being analyzed.

Figure 2—Incident Handling Process Diagram



Source: Teju Oyewole. Reprinted with permission.

Figure 3—Factors Cascade



Source: Teju Oyewole. Reprinted with permission.

IR Improvement
The ability of the IR personnel to properly predict or project what can be done in future occurrences based on the previous SA acquired leads to improvements in the IR process. Reviewing the lessons learned after an incident has taken place is an important activity. The techniques or approaches used in dealing with incidents, the response time and possibilities of better approaches are documented at this phase.

SA Application to IR Improvement
The best reasonable efforts of SA acquired from previous phases will turn out to be the best efforts in handling future incidents and events and may solve what-if questions.[9] The feedback from the SA will enhance the ability to effectively improve IR and other organizational processes. The strategic decisions that prevent a recurrence of similar incidents or improve the security capability of an organization are the results of tandem phases from SA.

Similarly, the application of SA in making strategic decisions in an organization is also validated by Morri's Semiotic Model as studied in ISACA's COBIT® 5 information model[10] in using three main components to manage and carefully select the useful information for effective business decisions:

- **Syntactic**—The structure of information; within the SA context, the perception or signs
- **Semantics**—The meaning of the information; within the SA context, the comprehension
- **Pragmatics**—The usage of the information; within the SA context, the projection

Each of the three main components influences one another in acquiring SA. However, there are other environmental and individual factors that can affect the SA process.

The environmental factors refer to the functions of the organization such as systems capabilities, interface design, stress and workloads, complexity, and automation (green arrow in **figure 1**). In real life, these can be security solutions and organization processes and procedures.

The individual factors are the abilities, experience and training of the IR personnel that underpin their performance (green arrow in **figure 1**).

These resultant factors can influence the IR personnel's information processing abilities in responding to every incident. An experienced IR person with soundly acquired SA can be influenced to make a bad decision if an input from environmental factors is not favorable. This integrated process is referred to as the "factors cascade" (FC) from environmental and individual factors through to the informed decision—the nucleus of an organization.

The FC in managing a security incident can be depicted as shown in the **figure 3**:

- Environmental and individual factors
- Incident alerts
- Situation awareness
- Informed decision

Advancing IR Process Through the SA Adoption

It is clear that SA can be an important factor in the success of an organization's information security IR process. What, then, can an organization do to try to improve the information security SA of its IR personnel? There are a number of efforts that can advance IR in an organization including:

- Establishing the awareness of the human factor implication in the enterprise security culture
- Developing information security self-efficacy as part of the personnel performance appraisal process
- Creating and adopting a new security culture that addresses human vulnerabilities
- Developing an IR process based on human behavior
- Establishing training and mentorship related to SA implications on IR

- Creating and implementing SA as part of the security layers across the organization
- Establishing that the IR process is the responsibility of everyone in the organization
- Conducting psychometry and SA scenario tests as part of yearly security drills
- Developing and maintaining a security policy that addresses SA for all personnel

To achieve IR advancement, the tasks listed can be incorporated in the organization's security programs through inclusion in the security policies, adoption of the listed efforts, and establishment of close monitoring and control to evaluate and review the progress. Studies suggest that SA measurement requires validity, which can be achieved through yearly drills of scenario tests of incidents with applicable and actionable responses within an allotted time.

Conclusion

In order to foster IR advancement, SA is critical in making timely and effective decisions during IR. This application can also serve as a top-layer control for other technical solutions.

Even with the most intelligent security solutions, the human factor remains a critical element that cannot be overlooked. The response to incident alerts is largely a function of the human factor; hence, a strong defense can be assured and an organization's security posture can move from "patch and pray" to security by default.

Endnotes

1 Galvez, S.; J. Shackman; I. Guzman; S. M. Ho; "Factors Affecting Individual Information Security Practices," *Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research*, June 2015, p. 135-144, *http://dl.acm.org/citation.cfm?id=2751966*

2 *Ibid*.

3 Endsley, M. R.; "Towards a Theory of Situation Awareness in Dynamic Systems," *Human Factors: The Journal of the Human Factors and Ergonomics Society*, vol. 37, no. 1, March 1995, *http://trid.trb.org/view.aspx?id=426377*

4 Gudmundsson, M.; R. Pedersen; K. Vogfjörd; B. Thorbjarnardóttir; S. Jakobsdóttir; M. Roberts; "Eruptions of Eyjafjallajökull Volcano, Iceland," *Eos*, vol. 92, iss. 21, 3 June 2011, p. 190-191, *http://onlinelibrary.wiley.com/doi/10.1029/2010EO210002/pdf*

5 Johnson, L.; *Computer Incident Response and Forensics Team Management: Conducting a Successful Incident Response*, Syngress, USA, 2014

6 *Op cit*, Galvez, *et al*.

7 *Op cit*, Johnson

8 *Ibid*.

9 Evangelopoulou, M.; C. W. Johnson; "Implementation of Safety Techniques in a Cyber Domain," ACM Digital Library, September 2014, *http://dl.acm.org/citation.cfm?doid=2659651.2659740*

10 ISACA, *COBIT® 5: Enabling Information*, USA, 2013, p. 37