Factors Influencing the Adoption of Cybersecurity Situational Awareness Programs

The rapid and sustainable advancement of the IT environment has improved domestic and industrial operations and connectivity. The risk to the security and safety of data in the cyberenvironment also increases and becomes more complex with the advancement of technology.[1] Concepts such as authentication, authorization and nonrepudiation have been applied to promote confidentiality, integrity and availability of data, but the risk remains significant.[2] Cyberattacks continue to occur at increasing rates and in different forms, including attacks from within victims' systems.[3] The focus of the research described herein is on academic organizations and to advance the adoption of cybersecurity situational awareness programs.

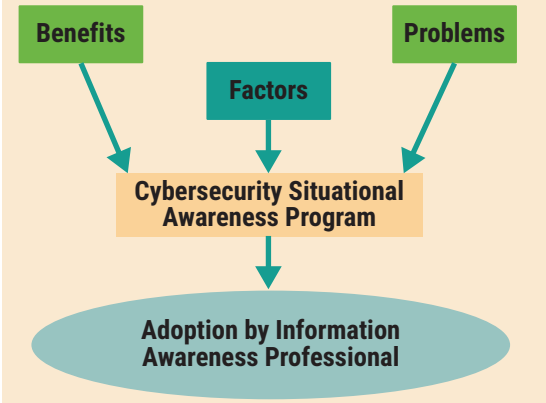
Even with the knowledge and skills possessed by many managers, there is still a failure to develop effective measures to address the risk of cyberattacks owing to the lack of partnership between developed and developing countries.[4] Lack of cooperation generates safe havens where cybercriminals take advantage of loopholes in the legal environment, particularly in developing nations, to commit cybercrime. As such, the legal environment is ineffective in addressing increasingly complex cyberthreats in almost every part of the world.[5] The adoption of cyber situational awareness programs by information assurance professionals is a possible solution to the observed inefficiency of preventing cyberattacks.

Situational awareness offers a basis for the prevention and effective response to cyberattacks and programs that target information assurance professionals. The occurrence of cyberattacks and the magnitude of financial losses resulting from attacks suggest a failure to adopt situational awareness programs or ineffective adoption. A study was conducted to investigate the adoption of cyber situational awareness programs and the factors affecting their adoption. The study sought to develop knowledge on the adoption of awareness programs and factors affecting adoption.

Conceptual Framework

A conceptual framework based on the accident model and process models was the foundation of the study (**figure 1**). Based on the conceptual framework, a phenomenon (in this case, a cyberattack) occurs due to the lack of constraints on a system.[6] Alternatively, constraints may exist, but a failure to enforce them adequately can lead to the occurrence of an undesired incident.[7]

Figure 1—Conceptual Framework



David V. Hart, Ph.D., CISM, CISSP, ITIL Foundation v3, Network+, Security+
Is an information assurance engineer with Amyx. He has more than 15 years of experience as a hands-on technologist specializing in cybersecurity and information assurance with large enterprise environments for institutions of higher learning and with the US Department of Defense. He plays a key role in secure implementation, addressing regulatory compliance and the process improvement of numerous major systems and applications for all his customers. Hart is an active member of the ISACA® Philadelphia (Pennsylvania, USA) Chapter, the (ISC)² Philadelphia chapter, and a long-standing member of the High Technology Crime Investigation Association (HTCIA) Delaware Valley/Philadelphia Valley Chapter.

Cyberattacks result from failures to adequately enforce constraints, for example, lack of partnership between developed and developing countries, inadequate security awareness programs, lack of security expertise, and poor response measures that cyber situational awareness could promote. Failure to adopt situational awareness programs can also result in weaknesses in controls for cybersecurity. Similarly, constraints may exist that prevent the adoption of cyber situational awareness programs and undermine their adoption and positive effect on cybersecurity. An understanding of the adoption of cyber situational awareness programs as a constraint to the occurrence of cybercrime and an understanding of factors to the adoption as other constraints were the focus of the study. Barriers to the acceptance and use of cyber situational awareness programs affect the adoption, and the adoption of the programs affects cybersecurity.

> “FAILURE TO ADOPT SITUATIONAL AWARENESS PROGRAMS CAN ALSO RESULT IN WEAKNESSES IN CONTROLS FOR CYBERSECURITY.”

Methodology

A qualitative phenomenological methodology was used in this study via an open-ended questionnaire. The phenomenology research method is used to explicate how human beings experience a particular phenomenon. In this study, the phenomenon is cybersecurity. Incorporating a qualitative research approach with a phenomenological study allowed for the discovery of additional insights that otherwise might go unnoticed by using a single methodological approach. The researcher designed the study to examine the “lived experiences” of each of the participants, which made phenomenology an appropriate research design.

A total of 17 participants were recruited for the study from the computer services department of five universities using purposive sampling. A purposive sample is chosen on the basis of the population characteristics and the study’s objective rather than probability. The population in this research study consisted of management and employees of the computer services department of the selected universities who have been employed by the department for at least two years. The sample participants were identified as either management or employee.

Data were collected using both interview and survey questionnaires. The interview questions were open-ended to allow the participants to describe their experiences in their own words. The researcher also took notes and made notations in the field journal. The survey questionnaire collected demographic information from the participants. Demographics included the participant’s job title, age, gender and number of years working at their current organization. The qualitative interview data were interpreted and analyzed using a thematic analysis method.[8]

Results

The main research question of the study centered on determining the factors affecting buy-in to the idea of adopting cybersecurity situational awareness and its factors, thereby presenting an opportunity to correct and prevent the identified rising threats to information systems. Five research

questions were then formulated to expound on and better address the central query of the study. **Figure 2** shows the themes that emerged from participant responses and the research question they addressed.

Influencing the Adoption of Cybersecurity Situational Awareness Programs

There were multiple needs that affected university adoption of cybersecurity situational awareness programs. There was a need by universities to protect pertinent records and information of end users (i.e., students, faculty members), thus the employment of information assurance professionals in the academic institutions. More specifically, professionals were recruited to better manage sensitive information such as personal records, health records and research data belonging to the schools or universities. There was a need to be cautious and vigilant to find security issues and threats. In addition, there was also a need to increase end users' awareness of cybersecurity. The change in the security system should start with the users themselves. They should be knowledgeable and careful as they access, manage and share their data. Once the needs are addressed, cybersecurity situational awareness programs in universities will be adopted, thereby helping to effectively deal with cybersecurity threats.

Systems for Protecting and Sharing Personal and Sensitive Information

Currently, at the universities presented in this study, there is a presence of campaigns against probable cyberattacks. The following approaches and methods have been performed and put into place:

- Basic Internet security policies (i.e., encryption of email, data protection, two-factor authentication, firewall, security software)

Figure 2—Themes and Research Questions

Research Question (RQ)	Theme
RQ 1: What are the needs and factors that influence the adoption of cybersecurity situational awareness programs by information assurance professionals in an academic organization?	**Major theme 1:** Protecting pertinent records and information of end users (i.e., students, faculty members) **Subtheme 1:** Managing sensitive information such as personal records, health records and research data **Minor theme 1:** Increasing end users' (i.e., students, faculty members) awareness of cybersecurity
RQ 2: What systems are currently in place for the protection and sharing of personal and sensitive information in the academic organization?	**Major theme 2:** Starting campaigns against probable cyberattacks **Subtheme 1:** Presence of basic Internet security policies (e.g., encryption of email, data protection, two-factor authentication, firewall, security software) **Subtheme 2:** Training and educating end users against probable cyberattacks **Subtheme 3:** Formalizing stricter and more proactive cybersecurity policies
RQ 3: What are the challenges perceived and obstacles discovered by information assurance professionals in the awareness of security threats to cybersystems' security in an academic organization?	**Minor theme 1:** Lacking a proactive approach in addressing cybersecurity issues **Subtheme 1:** Staying updated on and well-informed of the technological issues and advances
RQ 4: What are the roles and participation requirements of the end user, as perceived by information assurance professionals, in enhancing cybersecurity situational awareness in the academic organization?	**Major theme 3:** Playing a crucial and active role in enhancing cybersecurity situational awareness **Subtheme 1:** Needing end users' willingness to learn and be involved in the changes **Subtheme 2:** End users' actions and decisions may affect the whole network or system
RQ 5: How can current systems be improved to facilitate more efficient cybersecurity situational awareness of information assurance professionals and end users in the academic organization?	**Major theme 4:** Increasing end user training on and knowledge of how to protect themselves from cyberattacks **Minor theme 1:** Increasing communication across departments

> PROTECTING END USERS FROM SECURITY BREACHES AND MALICIOUS ATTACKS REQUIRES THE PROMOTION OF SITUATIONAL AWARENESS BY ALL THOSE WHO USE, OPERATE AND/OR EVALUATE THE SYSTEM.

- Training and educating end users against probable cyberattacks
- Formalizing stricter and more proactive cybersecurity policies

One of the first changes adopted by universities presented in the study was to secure emails received and forwarded by school personnel and students.

Challenges of Raising Awareness of Security Threats

From the study, the main challenge in raising the awareness of security threats is the fact that academic institutions' and their members' lack of proactiveness in addressing possible cybersecurity threats. The current attitudes and behaviors of the schools' stakeholders are still not enough to fully defend and protect themselves from cyberthreats and attacks. There is a perception that cybersecurity is not urgent or crucial.

End User Roles and Participation Requirements
End users play a crucial and active role in enhancing cybersecurity situational awareness. With the end users' lack of proactiveness, knowledge and attentiveness, data and information can be accessed easily and stolen by cyberattackers. There is a need for the end user to learn and be involved in the changes implemented through the awareness campaigns or programs. Moreover, end users' actions and decisions affect the whole network or system of the academic institutions. For instance, updating security firewalls, the use of spam and phishing detection measures, and adopting effective cybersecurity response mechanisms can determine whether a university information system is secure from cyberattacks.

Improvements to Current Systems
Some participants suggested the increase in training and knowledge of end users on how to protect themselves from probable cyberattacks. The current systems seemed to facilitate better cybersecurity situational awareness by increasing the programs and activities that target the education of end users. Programs should be more creative and interactive to catch the attention of users and encourage end-user participation.

Implications of Study on Academic Institutions

Multiple individuals play critical roles in the promotion of a secure cybernetwork, which includes appropriate cybersecurity measures of all end users, software and hardware. Protecting end users from security breaches and malicious attacks requires the promotion of situational awareness by all those who use, operate and/or evaluate the system. Cybersecurity departments should use the insights from this study and adopt cybersecurity situational awareness programs to facilitate more efficacy among information professionals, end users, and leaders and managers within academic institutions. While this study was mainly intended for academic institutions, findings can still be applied in other organizations that seek to better their cybersecurity measures.

From the current study, the researcher has established that there are several gaps in the available literature regarding the protection of end-user data within academic institutions, and there are several perceived obstacles, barriers and challenges to the maintenance of a secure system within this organizational context. There is a need for further guidance on how to improve cybernetworks' weaknesses such as low situational awareness or limited system constraints in academic institutions to increase their security and fill a significant gap in the literature pertaining to cybersecurity.

Policy makers in academic institutions can use the results of the study to protect end users from having personal data stolen or exposed to a malicious attack. Specifically, universities and system developers need to incorporate the concept of situational awareness into their designs to prevent compromising any protective system constraint. Accordingly, policy within the information technology field must also incorporate the concept of situational awareness to continue to develop this quality among professionals who design cybersecurity networks within academic environments.

> “EACH END USER SERVES AS A CONSTRAINT WITHIN A CYBERNETWORK, AND LOW SITUATIONAL AWARENESS AT ONE POINT WITHIN THIS SYSTEM CAN COMPROMISE THE ENTIRE NETWORK.”

The results indicate how end users of common public cybernetworks are exposed to relatively high and consistent threats of security breaches and malicious attacks. This is due to exposure of vulnerabilities owing to the lack of cybersecurity situational awareness programs in academic institutions. Despite having some baseline security measures, common practices and low situational awareness make the use of public networks increasingly high, which exposes end users to the vulnerabilities of cyberattacks. There is a need for greater situational awareness among academic institutions to protect against breaches, theft of personal information and malicious attacks. Each end user serves as a constraint within a cybernetwork, and low situational awareness at one point within this system can compromise the entire network. This calls for the adoption of cybersecurity situational awareness programs not only in academic institutions, but also any other organization looking to mitigate cybersecurity threats. Cybersecurity is a common concern for organizations that use information systems, which implies that the recommendation for adoption of programs meant to better information system security can be applied to other organizations facing such threats.

Conclusion

The purpose of this research was to focus the need for academic organizations to advance the adoption of cybersecurity situational awareness programs. The results offer support for the study’s conceptual framework, suggesting that increasing constraints placed on organizational systems can increase that system’s integrity through multiple channels. Increasing constraints involving education and training, leadership, management, willingness on the part of organizational members, and communication are critical factors that may lead to improved protection of end users within academic institutions.

Endnotes

1 Singer, P. W.; A. Friedman; *Cybersecurity and Cyberwar: What Everyone Needs to Know*, Oxford University Press, USA, 2014
2 Graham, J.; R. Olson; R. Howard; *Cyber Security Essentials,* CRC Press, USA, 2010
3 Shackelford, S.; *Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace*, Cambridge University Press, USA, 2014
4 *Ibid*.
5 Proia, A.; D. Simshaw; K. Hauser; “Consumer Cloud Robotics and the Fair Information Practice Principles: Recognizing the Challenges and Opportunities Ahead,” *Minnesota Journal of Law, Science & Technology*, vol. 16, 2015
6 Zhou, J.; K. Li; Z. Luo; S. Ma; “Railway Accident Analysis Using Information Theory and Complex Network,” 2013 International Conference on Industrial and Management Science, 2013, p. 865-876

7 Adeola, F.; *Industrial Disasters, Toxic Waste, and Community Impact: Health Effects and Environmental Justice Struggles Around the Globe*, Lexington Books, USA, 2012
8 Nowell, L. S.; J. M. Norris; D. E. White; N. J. Moules; "Thematic Analysis: Striving to Meet the Trustworthiness Criteria," *International Journal of Qualitative Methods*, vol. 16, 2017, p. 1-13