Information Security Management in University Campus Using Cognitive Security

Roberto Omar Andrade
roberto.andrade@epn.edu.ec
Escuela Politécnica Nacional

Quito, Ecuador

Susana Cadena
scadena@uce.edu.ec
Universidad Central del Ecuador

Quito, Ecuador

Luis Tello-Oquendo
luis.tello@unach.edu.ec
Universidad Nacional de Chimborazo
Riobamba, Ecuador

Iván Ortiz Garcés
Ivan.ortiz@udla.edu.ec
Universidad de las Américas
Quito, Ecuador

Walter Fuertes
wmfuertes@espe.edu.ec
Universidad de las Fuerzas Armadas ESPE
Sangolquí, Ecuador

Alyssa Cadena
akcadena@espe.edu.ec
Universidad de las Fuerzas Armadas ESPE
Sangolquí, Ecuador

Daniela Córdova
daniela.cordova@epn.edu.ec
Escuela Politécnica Nacional
Quito, Ecuador

María Fernanda Cazares
mcazares@ups.edu.ec
Universidad Politécnica Salesiana
Quito, Ecuador

Abstract

Nowadays, most universities offer free Internet connections, access to scientific databases, and advanced computer networks for the members of their community, which generates dynamic and complex scenarios. In this context, it is necessary to define proactive security strategies, as well as the integration of technology and research. This work presents a general vision of the experience adopted by the universities in the field of information security management using cognitive security.

Keywords: Security Operation Center, Cognitive Security, Big Data, Incident Response Team.

1. INTRODUCTION

University faces necessary changes due to the technological disruption of the last years. The use of information and communication technologies (ICTs) in the classroom raises new educational models that strengthen the interactive and collaborative work between teacher and student. The teacher can share a document with the group of students who can edit it simultaneously and discuss its content. For doing so, there is no need to be in the same physical space; the interaction can be performed by video-conference and email collaboration services housed in public clouds. The teacher can validate in real-time the existence of plagiarism and send feedback before the final grade.

On the other hand, the ability of students and teachers to access scientific bibliographic resources from around the world allows enriching the theoretical and practical content embodied in the classrooms. Having access to scientific databases such as Scopus, ACM, IEEE or Web of Science has become an invaluable tool that helps understand science and technology from a

global perspective; this fact pushes the generation of entrepreneurship and innovation in the university.
Furthermore, access to the Internet is considered one of the most significant enablers of the change in traditional education models [1]. The social-technological model generated by a daily behavior against the use of technology, and the accessibility to the Internet, poses new challenges on how to define information security strategies.

Information security management in universities should be considered as a new scenario (hyper-connected world), where students could have two or three devices from which they access to Internet, share workbooks through the use of groups in social networks, search for educational resources that are geographically dispersed, and use of large audio and video files in real-time in classrooms.

Regarding the security of information, universities face security problems in recent years, such as:

- Unauthorized access;
- Denial of service attacks;
- Servers with malware;
- Injection of malicious code.

The adoption of technological solutions such as Big Data, Cloud, Internet of Things (IoT), and bring your own device (BYOD), improves the services to the members of the university community but generates more dynamic and complex scenarios that strongly impact the security of information. This has prompted new strategies to defend cybersecurity. The security team of the universities establishes response actions to deal with the security attacks generated from the security personnel's experience, and many of the times this generated knowledge is lost because it is not documented after the resolution of an incident.

Following good security practices, the use of lessons learned to defend against new attacks is essential to reduce response times. In this context, the idea is to propose the use of recommender systems so that the security team can access the most appropriate response actions to resolve a security incident based on the use of previously generated knowledge and take advantage of the experience and collaboration between members of the security team. In order that the recommender system is not an isolated tool, an organizational model is proposed in which the research processes, including new technologies and incident response, take advantage of the cognitive processes inherent to the generation of knowledge and decisions making; for which as an enabler of the organizational model proposal we consider the application of cognitive security.

The remainder of this work is organized as follows. Sections 2 and 3 present an analysis of the emerging technologies and security challenges that these technologies are generating, which implies a change to traditional security models. Section 4 presents the security organization model proposed by the universities. Section 5 describes the contribution of establishing an academic computer security incident response team (CSIRT) and its components are mentioned comprehensively. Finally, Section 6 presents the conclusions with the respective contributions of this work.

2. EMERGING TECHNOLOGIES THAT CHANGE SECURITY MODELS

Universities, under the approach of "Open University", have considered the implementation of technological solutions that allow providing functionalities such as access to the Internet, mobility, interconnection with other universities in the world, high-speed access, and security that are required by the members of the university community (i.e., teachers, students, administrative, visitors). In Figure 1, we present the leading technologies adopted by the universities on this matter.

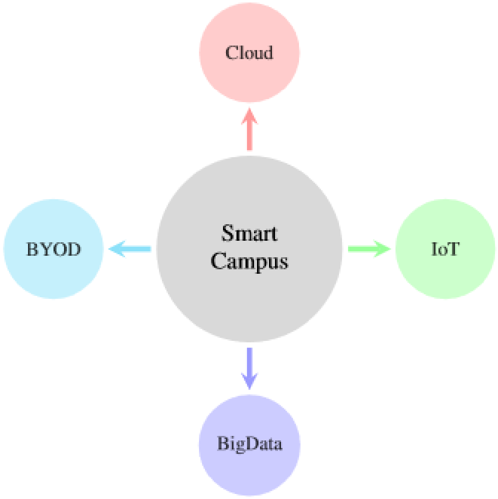

FIGURE 1: Emerging Technologies in the University.

Regarding the use of cloud solutions, it was considered bearing in mind the availability, flexibility, and scalability characteristics of this solution. Some cloud solutions considered by the universities are:

- Infrastructure as a Service - IAAS, to provide resources of virtual machines to teachers and students for experimental use or, from the universities perspective, as a customer of the service for the redundancy and contingency of institutional web portals.
- Software as a service - SAAS, to provide the use of software in the campus model for the development of experimental work or to have collaboration tools such as videoconferencing or email.

The adoption of the Cloud has generated the universities to ask the following questions related to the management of security:

- How to establish user authentication to these new services outside the universities?
- How to manage the privacy of information in the Cloud?
- How to establish information backup processes in the Cloud?

BYOD is a technological model in which students bring their device to school for accessing to ICTs resources, but new challenges were generated for the security of the information of the universities in these scenarios, among which we can mention:

- How to establish user authentication in different technological devices?
- How to handle the traceability processes of the connections made without invading the privacy of the user?
- How to define high redundancy and scalability schemes to support about 10 thousand users, which on average can have at least one technological device?
- How to verify the use of antivirus before access to the data network?

In the case of IoT deployment, it should be considered that deploying this type of networks usually means that the devices do not handle authentication processes. As a new challenge for universities, IoT identity management schemes should be considered.

Finally, in the case of Big Data, it is necessary to understand that information is extracted from different sources of information; then, two key factors that have become challenges for the universities should be considered:

- Confidentiality of information;
- The integrity of the information.

In this case, two strategies are applied:

- Use of confidentiality agreements;
- Data quality processes.

Universities have to solve daily information security problems related to attacks in order to guarantee the availability and integrity of the ICT services that are used by the university community. Table I presents a consolidation of the most common attacks in the universities and their percentage [7].

TABLE 1: Most Common Attacks in Universities.

Attacks	Percentage
Defacement	50
SQLi	20
DNS Poisoning	10
Account Hijacking	5
Exploit Vulnerabilities	15

Aiming at handling these attacks, security solutions such as firewalls, intrusion prevention systems (IPSs), redundancy systems, event correlation systems, and antivirus solutions have been strengthened in the universities. However, the adoption of new technologies has generated new vulnerabilities and gaps that can be exploited by attackers daily, which has led to identifying which are the new challenges that must be faced to establish new security defense strategies.

3. COGNITIVE SECURITY ORGANIZATION MODEL PROPOSAL

Our Cognitive Security Organization Model proposal considers some components to establish an adequate process in the management of information security, which allows to face problems for proactive defense. The organizational model includes two main components:

1) Security strategies;
2) Enablers to execute the strategies.

Figure 2 depicts the components and elements that make up the organizational information security model currently proposed in the universities.

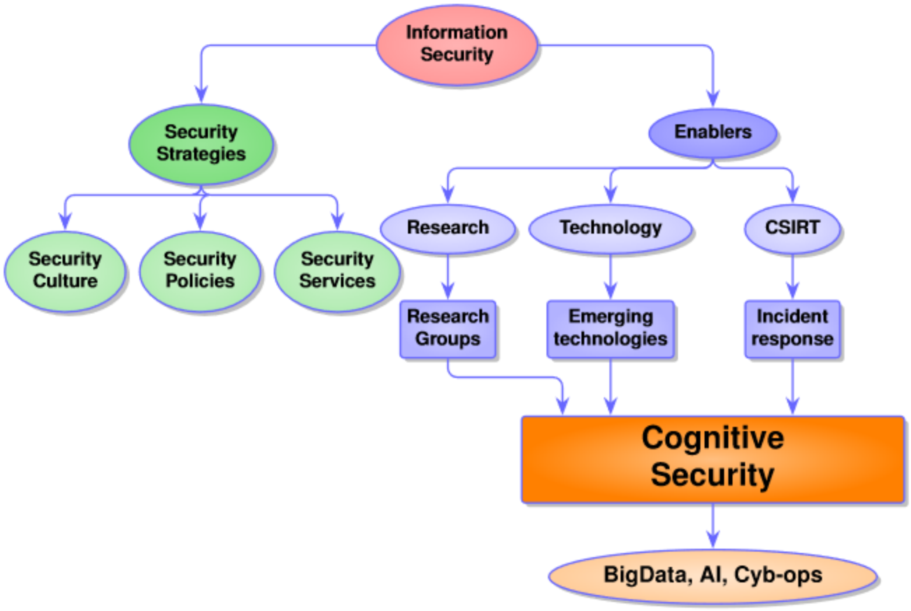

FIGURE 2: Cognitive Security Organization Model Proposal.

3.1 Security Strategies

1) Security Culture: The proposed model considers that security culture is the responsibility of all members of the university, so it establishes a strategy to generate that students, professors, and administrative staff perceive cybersecurity from their role and perspective. For this is necessary that students understand that the inadequate use of institutional computing resources can have legal implications, teachers perform the proper process of managing institutional credentials to access the different technological services and under no circumstances loan credentials because of the implications of the modification of information especially in educational systems. At the administrative level, it has been sought that the management of information is carried out under the principles of confidentiality and the processes of integrity and quality of the information that is used for the administrative processes related to the members of the university are enhanced.

2) Security Policies: The administration of information security requires the establishment of policies that institute the appropriate behavior of each member of the university related to the proper use of technological resources and information. In the case of the universities, the approval of policies is carried out by the highest collegiate body, the University Council, for which a general security policy has been approved and from this about 23 security directives have been created. Among them we have:

- Classification and access to information;
- Security guidelines computer network;
- Guidelines for handling passwords;
- Guidelines for antivirus management;
- Guidelines for backup, protection and retrieval of information;
- The standard for the creation of user accounts.

3.2 Security Services

The following are considered as security services:

- Classification and access to information;
- Security guidelines network;
- Guidelines for handling passwords;
- Guidelines for antivirus management;
- Guidelines for backup, protection, and retrieval of information;
- The standard for the creation of user accounts.

Also, three kinds of services are identified as follows:

1) Reactive Services:
- Incident management;
- Vulnerability Management.

2) Proactive Services:
- Technological surveillance;
- Security audits or evaluations;
- Development of security tools.

3) Security Management:
- Training.

The human being is considered the weakest link in the security chain; for this reason, training the user is one of the most critical strategies in security. In this specific issue, the universities have not only focused on the technical training of the CSIRT team but have also considered the scope of the different members of the university community. The content of the training focuses on good security practices, such as phishing detection, the use of antivirus, the identification of malicious mail, the use of strong passwords, and clean desk procedures.

4. CSIRT-UNIVERSITIES

Some organizations establish as a security strategy the creation of a security incident response team (CSIRT), which consists of a specialized group of security experts in both the technical and legal fields to be able to resolve attacks that have compromised the security of information [3]. There are different types of CSIRT in the commercial, military, business, and academic fields.

Academic CSIRTs are generally established in universities, and their functioning differs from the others since they actively promote the processes of technological observation and research to strengthen the generation of procedures, software, and training focused on the handling of security incidents.

Universities have set up a CSIRT aiming at having a specialized team of professionals who focus specifically on establishing information security strategies to be adopted by the universities to minimize the impacts and risks of attacks that affect the cybersecurity of the institution. In the CSIRT-Universities, three macro objectives have been proposed:

- Detect, identify and technically support the university community in the handling of computer security incidents;
- Detect and investigate computer security threats;
- Publish the results and research of the institution that are related to the management of the CSIRT.

The following are the basic components of the CSIRT [7]:

A. Staff

In order to perform security management and incident management processes, the following personnel is required as minimum:

- Team leader / coordinator;
- Responsible for systems and information security;
- Communication or public relations team;
- Classifier or triage;
- Incident management team - second level;
- Legal team.

B. Infrastructure

The CSIRT requires an infrastructure that allows to carry out its management processes independently of the technology unit. This infrastructure will also allow the analysis of malicious emails or malicious software without affecting the institutional information systems. The minimum infrastructure required in the CSIRT is the following [5]:

- Management system for requirements;
- Incident log system;
- Servers for monitoring services and applications;
- Servers for malicious code analysis;
- Independent Internet access.

C. Training

The following training courses are defined (as a minimum) to strengthen the technical skills of the CSIRT staff:

- Forensic analysis;
- Handling of event correlation tools;
- Penetration testing techniques;
- Information security regulations.

D. Certification

To keep the staff and processes of the CSIRT in continuous improvement, certification in FIRST can be established as an objective. To maintain the membership, it is necessary to meet specific requirements such as:

- Updated policies;
- Maintenance of security infrastructure;
- Periodic staff training.

E. External relations

The operation of the CSIRT requires the establishment of external relations that allow having alerts or security bulletins to be informed. Sometimes, it is necessary to have this additional support to resolve security incidents that may exceed the knowledge of the CSIRT staff.

F. Research lines

The academic CSIRT must be directly related to research projects that support the improvement of the processes and tools used when handling security incidents:

1) Institutional Encryption;
2) Institutional Antibot;
3) Botnet vulnerability analysis;
4) Analysis of institutional Malware, collection, sample, classification, and statistics;
5) Intelligent log analysis software to detect malicious traffic: Http scans, https scans;
6) Vulnerability analysis defacement;
7) Data mining and/or algorithms focused on web 2.0;
8) Automatic generation of computer security testing rooms or rooms.

5. COGNITIVE SECURITY COMPONENT

Based on the literature review, business solutions, and approaches of internationally recognized companies in the field of technology related to cognitive security, we define cognitive security as the ability to generate cognition for efficient decision making in real-time by the human or a computer system. This can be done based on the perception of cybersecurity that the computer system generates from its environment (situational-awareness) and the knowledge about itself (self-awareness or insights), through the analysis of any type of information (structured or unstructured) using artificial intelligence techniques (data mining, machine learning, natural language processing, and human-computer interaction) and data analysis (big data, processes stochastics, game theory) emulating the human thought process for continuous learning, decision making and security analysis.

The goal of the recommender system is to provide an overview of the state of the university cybersecurity from a cognitive approach; therefore, we consider the three phases of the cognitive processes as illustrated in Figure 3.

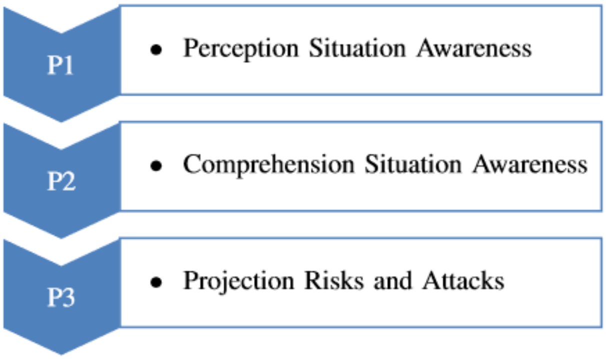
P1
• Perception Situation Awareness
P2
• Comprehension Situation Awareness
P3
• Projection Risks and Attacks

FIGURE 3: Cybersecurity Cognitive Phases.

Recommender systems (RS) or decision support systems (DSS), according to Holsapple and Clyde [6] can be classified into six frameworks: text-oriented, database-oriented, spreadsheet-oriented, solver-oriented, rule-oriented, and compound. Hybrid DSS containing at least two of the mentioned frameworks provide better knowledge for decision making.

Proposals for decision-making models in cybersecurity can be based on [7-12]:

- Fuzzy decision making and risk assessment;
- Ontologies-Based;

- Hierarchical task network planning;
- Risk impact tolerance;
- Attack damage costs;
- Markov decision.

Recommender systems can be classified into four types, which are shown in Figure 4.

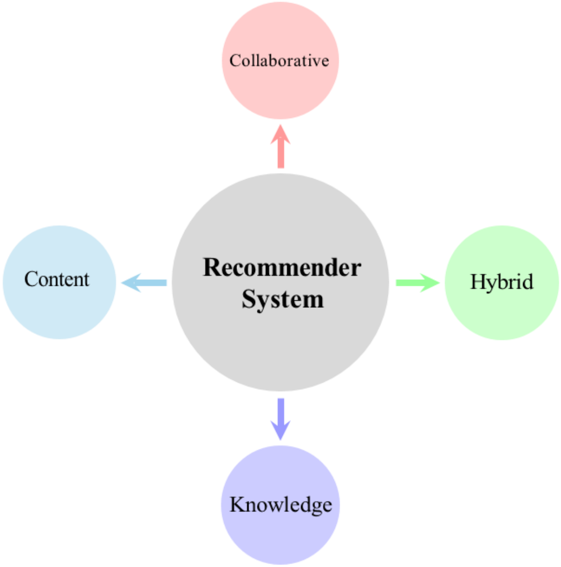

FIGURE 4: Recommender System Types.

In Table 2, we present the main characteristics of the recommender systems. Generally, the most common use of the recommender systems is focused on services to consumers; therefore, it is necessary to adapt it to the cybersecurity context. The systems based on collaboration and content require the monitoring of user actions and collection of rankings. For doing so, it is necessary to consider the implementation of a data warehouse and consider the privacy aspects.

TABLE 2: Recommender Systems Attributes.

Type	Attribute	Typical Application	Method	Data
Collaborative	User-item matrix	Customer purchase	Pearson's correlation	Track user actions Collect ratings
Content	Similarity Item	Customer purchase	K-nearest-neighbor	Track user actions Collect ratings
Knowledge	Similarity Item	Customer purchase	Instance-Based Learning	Features Items

In general terms, the proposed recommender system (see Figure 5) considers the interaction with the members of both the CSIRT of the university and the national CSIRT. It proposes a data warehouse for the maintenance of the actions of the agents and logs of the computer systems and allows the integration with security solutions like SIEM and firewalls.

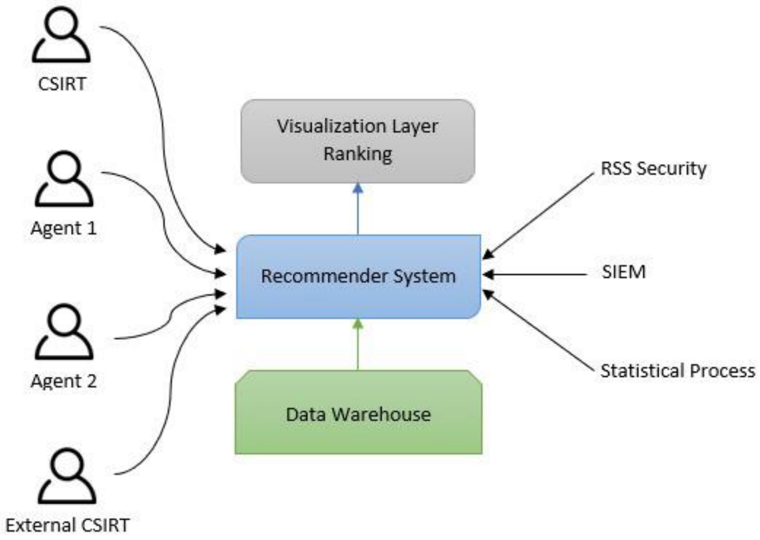

FIGURE 5: Cybersecurity Recommender System.

Specifically, we propose a hybrid model in order to establish an accurate situational awareness. This recommender system is aligned with the decision phase of the OODA model and supports the cognitive process of projection to establish the future state of the cybersecurity situation awareness [13]. The proposed recommender system consists of three layers: modeling, processing, and presentation. In the following, we describe each layer briefly.

A. Modeling

This layer is related to the orientation phase of the OODA model and it allows to execute the cognitive process of comprehension. For doing so, it establishes a correlation of dependence of different security aspects such as vulnerabilities, threats, risks, and attacks, which allows establishing a more accurate and real situational awareness based on solid facts.

To establish the dependency matrix, we propose the use of at least the following security analysis models:

- Vulnerability model;
- Threat model;
- Attack model;
- Impact model;
- Planning model;
- Risk model.

B. Processing

In this layer, the cybersecurity situation awareness is established; the CSIRT team can select for different models considering the following contexts:

- Intelligence-Driven;
- Data Driven;
- Goal Driven;
- Knowledge-Driven.

C. Presentation

In this layer, the visualization for the security team is established, through visual representations such as attack graphs, commonly detected vulnerabilities, and the recommendations with the highest score obtained based on the observations of the different agents.

6. CONCLUSIONS

Different emerging technologies, together with different behavioral controls, bring as a consequence an adequate safety culture within organizations. However, higher educational institutes depend on technical security controls and ignore the adherence of end-users to the information security policies implemented to guarantee the security of institutional resources. The lack of end-user training concerning security incidents and institutional security policies results in security breaches and legitimate damage to information. Nowadays, there is a need to prepare university employees to realize the intensity of a possible deterioration of resources in the face of a security incident. The provision of policies and periodic monitoring can play a vital role in the protection of resources. The basis for an effective recommender system consists of three main components: modeling, processing, and visualization. The hybrid model permits to handle the attribute from content, collaboration, and knowledge types. If the recommender system is based on using the knowledge generated about security, it is possible to take advantage of the lessons learned and establish adequate and quick response actions.

7. ACKNOWLEDGMENT

The authors would like to thank the financial support of the Ecuadorian Corporation for the Development of Research and the Academy (RED CEDIA) in the development of this work, under Research Team GT-II-2017.

8. REFERENCES

[1] B. Collis and M. van der Wende, “Models of technology and change in higher education: an international comparative survey on the current and future use of ICT in higher education”. Netherlands: Center for Higher Education Policy Studies (CHEPS), 2002.

[2] BBC News. (2019). Students blamed for college cyber-attacks. [online] Available at: https://www.bbc.com/news/education-45496714 [Accessed 27 Jul. 2019].

[3] K. Moller, “Setting up a grid-cert: experiences of an academic CSIRT” in¨ Campus-Wide Information Systems, vol. 24, no. 4, 2007, pp. 260–270.

[4] Tello-Oquendo, L.; Tapia, F.; Fuertes, W.; Andrade, R.; Erazo, N.; Torres, J. and Cadena, A. (2019). A Structured Approach to Guide the Development of Incident Management Capability for Security and Privacy. In Proceedings of the 21st International Conference on Enterprise Information Systems - Volume 2: ICEIS, ISBN 978-989-758-372-8, pages 328-336. DOI: 10.5220/0007753503280336.

[5] Cadena, A., Gualoto, F., Fuertes, W., Tello-Oquendo, L., Andrade, R., Tapia, F., & Torres, J. (2019). Metrics and Indicators of Information Security Incident Management: A Systematic Mapping Study. Developments and Advances in Defense and Security, 507–519. DOI:10.1007/978-981-13-9155-2_40.

[6] C. Holsapple, “DSS architecture and types”, Decis. Support Syst., vol. 1, pp. 163–189, 01 2008.

[7] S. Berenjian, M. Shajari, N. Farshid, and M. Hatamian, “Intelligent automated intrusion response system based on fuzzy decision making and risk assessment,” in 2016 IEEE 8th International Conference on Intelligent Systems (IS), Sept 2016, pp. 709–714.

[8] V. M. Lanchas, V. A. V. Gonzalez, and F. R. Bueno, “Ontologies-based automated intrusion response system,” in Computational Intelligence in Security for Information Systems 2010, 2010, pp. 99–106.

[9] C. Mu and Y. Li, “An intrusion response decision-making model based on hierarchical task network planning,” Expert Systems with Applications, vol. 37, pp. 2465–2472, 03 2010.

[10] A. Shameli-Sendi and M. Dagenais, “Arito: Cyber-attack response system using accurate risk impact tolerance,” International Journal of Information Security, vol. 13, no. 4, pp. 367–390, Aug 2014. [Online]. Available: https://doi.org/10.1007/s10207-013-0222-9.

[11] A. Shameli-Sendi, H. Louafi, W. He, and M. Cheriet, “Dynamic optimal countermeasure selection for intrusion response system,” IEEE Trans. on Dep. and Sec. Comp., vol. 15, no. 5, pp. 755–770, Oct 2018.

[12] S. Iannucci and S. Abdelwahed, “Model-based response planning strategies for autonomic intrusion protection,” ACM Trans. Auton. Adapt. Syst., vol. 13, no. 1, pp. 4:1–4:23, Apr. 2018. [Online]. Available: http://doi.acm.org/10.1145/3168446.

[13] Andrade, R., Torres, J., & Flores, P. (2018). Management of information security indicators under a cognitive security model. 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC). DOI:10.1109/ccwc.2018.8301745.