4-1-2022

MANAGING CYBER HYGIENE AT A HIGHER EDUCATION INSTITUTION IN THE UNITED STATES

Shetia Butler Lamar
Savannah State University, Butlers@savannahstate.edu

MANAGING CYBER HYGIENE AT A HIGHER EDUCATION INSTITUTION IN THE UNITED STATES

Shetia C. Butler Lamar
Savannah State University
butlers@savannahstate.edu

ABSTRACT

Higher education institutions are obligated to protect their critical data, IT assets, and infrastructures. State governed institutions develop policies and procedures based on state mandated guidelines. While policies and procedures are updated regularly, cyber hygiene is managed in a manner that is feasible financially and based on personnel resources.

Savannah State University struggles with maintaining cyber hygiene given its need to manage state funding in a manner that supports operational and mandated costs, but also indirect costs like those that support cybersecurity.

The Holistic Cybersecurity Maturity Assessment Framework (HCYMAF) was deployed in this study to examine cybersecurity maturity and hygiene at Savannah State University (SSU). Findings indicate that SSU is currently operating at the minimum level of the HCYMAF and needs to consider action proposed in this study to promote higher levels of cyber maturity. This research contributes to the extant literature on cyber hygiene and maturity in higher education.

KEYWORDS

cybersecurity, cybersecurity maturity, cyber hygiene, Holistic Cybersecurity Maturity Assessment Framework

INTRODUCTION

The Holistic Cybersecurity Maturity Assessment Framework (HCYMAF) is formatted electronically and as an adaptable Microsoft Excel Workbook and Microsoft Word Document. The Microsoft versions of the instrument are accessible online for download and includes a section to report basic organizational information, guidance on how to use the instrument, and relevant questions related to each of the National Institute of Standards and Technology (NIST) Cybersecurity Framework; which support organizations ability to understand, manage and reduce cybersecurity risk by creating cybersecurity plans that successfully address the following 5 overarching domains: identify, protect, detect, respond, and recover.

The HCYMAF was designed to address the absence of a security maturity model specifically tailored for Higher Education Institutes (HEIs) (Aliyu et al, 2020). It considers existing work on maturity models and has adapted several of the existing models for the development of a Higher Education Institutes (HEI) Maturity Assessment. Based on applicability, the following models and standards were specifically considered in the development of the HCYMAF: the Capability Maturity Model (CMM), ISO/IEC 27001 Information Security Management, Citigroup's Information Security Evaluation Model (CITI-ISEM), U.S. Cybersecurity Capability Maturity Model (C2M2), National Initiative for Cybersecurity Education's Capability Maturity Model (NICE-CMM), Conceptual Design of a Cybersecurity Resilience Maturity Measurement (CRMM) Framework, and the Advancing Cybersecurity Capability Measurement using the CERT-RMM Maturity Indicator Level Scale.

The HCYMAF supports the assessment of the maturity of 15 specified domains to identify the strength of cybersecurity practices. Although the framework was designed to address the specified domains, the authors indicate that it can be easily extensible and adaptable to accommodate the incorporation of other domains or appropriate standards based on other geographical regions as needed (Aliyu et al, 2020). The Holistic Cybersecurity Maturity Assessment Framework (HCYMAF) domains are shown in Figure 1 below:

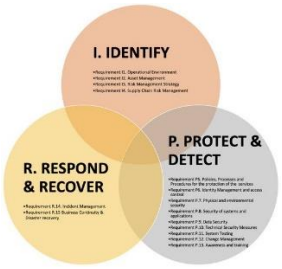

Figure 1. Holistic Cybersecurity Maturity Assessment Model

DESCRIPTION OF THE PROBLEM

With the rise in cybercrimes, there has recently been a rise in higher education cybersecurity attacks. Therefore, it has become more vital for institutions to evaluate their relevant policies and procedures to identify and employ appropriate policies, tools, and best practices to promote effective cybersecurity methods and cyber hygiene. While, state governed higher education institutions have an obligation to employ certain policy and procedural frameworks imposed by their governing bodies, they also have the flexibility to evaluate and employ their own approaches to maintaining the security of their assets. In order to maintain favorable levels of cyber hygiene, Savannah State University needs to reevaluate its current approach to cybersecurity to address current trends in cybersecurity attacks and promote favorable levels of awareness and support of its cyber hygiene.

LITERATURE REVIEW

Cyber hygiene is a fundamental term referring to cybersecurity best practices that an organization's security personnel and users apply to promote favorable health of hardware, software and other network systems and resources (Cain, Edward, and Still, 2018). Previous literature suggests that cyber hygiene helps to promote changed human behavior to support a more secure cyber environment (Maennel, Mäses, & Maennel 2018).

Other research suggests that the rise of higher education cyber-attacks promotes the need for the evaluation, maintenance and development of cyber security strategies and best practices (Zalaznick, 2013; Woody & Creel 2021; Kim & Beuran, 2018). The extant literature offers a number of resources to evaluate cybersecurity threats, policies, and cyber hygiene behaviors (ALEXEI and ALEXEI, 2021; Cain, Edward, and Still, 2018; Maennel, Mäses, & Maennel, 2018; Such et al, 2019; Ulven, & Wangen, 2021). However, the Holistic Cybersecurity Maturity Assessment Framework (HCYMAF) offers a comprehensive means by which to review and evaluate higher education institutes' current cyber security policies in relationship to relevant federal standards and frameworks to determine alignment and to identify weaknesses and strengths (Aliyu et al, 2020).

With regard to relevant policies, the extant literature also offers numerous resources to be considered by higher education institutes with regard to establishing best practices (SSU, USG, Cybersecurity Considerations for Institutions of Higher Education, Data Security: K-12 and Higher Education, Norris et al, 2019; Othmana, Rahimb, & Sadiqc; Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, Slonka, 2020; Ulven & Wangen,2021; US Department of Education; Woody & Creel; 2021).

METHODS

A phased insider action research approach was applied to this study (Coghlian, 2001). In the first phase, information about SSU's cybersecurity policies and practices was gathered from various published resources and through informal discussions with SSU's IT personnel who served as mentors on this project. The project mentors include SSU's Interim Chief Information Officer (CIO), Executive Director of Information Technology Services and Network Security Officer.

In phase two, in consideration of the information gathered about the university, fundamental guidance gained from the analysis of cyber hygiene and related approaches and offered in review of the Program Protection Plan (PPP) (DoD, 2020), the Holistic Cybersecurity Maturity Assessment Framework (HCYMAF) approach was adapted to align with FERPA, HIPPA, and USG\Board of Regents standards.

The HCYMAF was employed in phase 3 as a guideline for assessing and auditing Savannah State University's compliance with higher education related security regulations, privacy regulations, and best practices. The results of this review offered information about SSU's current cyber hygiene which was used in the final phase (Phase 4) of this study to ascertain appropriate recommendations for enhancing cyber hygiene based on the researcher's expertise as gained from relevant course studies and practical experience in cybersecurity management.

DELIVERABLES

The information gathering process resulted in the identification of areas of concern based on deployment of the Holistic Cybersecurity Maturity Assessment Framework (HCYMAF) approach to evaluate organizational cyber security hygiene.

This project had three primary deliverables: [1] to develop an adapted version of the HCYMAF that is relevant to higher education institutions in the US, [2] to produce a project report reflecting the assessment of SSU's cybersecurity maturity and cyber hygiene based on application of the HCYMAF, and [3] to propose a set of possible recommendations for enhancing SSU's cybersecurity maturity and cyber hygiene.

IMPLEMENTATION OF PROJECT

Information Gathering and Discovery

The initial phase of this research was primarily focused on obtaining more information about SSU's Cybersecurity policies and practices, gaining access to the HCYMAF instrument, and gathering information about FERPA, HIPPA, and USG\Board of Regents standards. To facilitate this discovery process, IT Department project mentors at SSU were contacted to gather information. Also, the authors of the HCYMAF research were contacted to request a copy of the HCYMAF instrument. And, research was conducted on the FERPA, HIPPA, and USG\Board of Regents standards online. Findings regarding each item are included in the sections below.

SSU's Cybersecurity Policies and Practices

Based on the information gathered from the project mentors from SSU's IT department, several discoveries were made. The discoveries are outlined in the paragraph below.

The university's current has only one cybersecurity personnel (ITS org structure). SSU's policies & procedures are published online on the university's website (SSU's Policies & Procedures). SSU's common types of attacks include: spam, virus, phishing attempts, copyright violations (students), system vulnerability exploitations from threat actors. SSU's mitigation and remediation techniques are accessible online via the security incident and response policy section of the university's Cybersecurity policies. SSU's Contingency plan can be found on the USG Cybersecurity website. The cybersecurity tools SSU uses include: Malwarebytes, OPSWAT/SafeConnect NAC, SANS, Securing the Human, Tennable Nessus, Cisco NGFW, Cisco VPN access, Cisco Firepower, Dell SecureWorks vulnerability scanner, Cisco DUO Multi-Factor Authentication, Office365 anti-spam, and a host of other security best practice procedures that the networking department employ, i.e. cloud backups, single sign-on, etc.

With regard to the university's governing body, the USG IT Handbook contains a wealth of information that SSU follows as a guide. The USG it Handbook is accessible online. The USG employs a Quarterly Cybersecurity Program Review Questionnaire to assess USG schools' cybersecurity policy implementation in alignment with USG standards.

Holistic Cybersecurity Maturity Assessment Framework (HCYMAF)

Dr. Aliyu who is one of the authors of the HCYMAF was contacted to gain access to the HCYMAF instrument. He provided direction to the site where the instrument could be accessed. The electronic version of the HCYMAF is the sole property of the UK's National Cyber Security Center (NCSC) based on a grant project. However, an MS Excel version of the instrument is accessible online. Users can register online to access and download a copy of the instrument. The Excel workbook of the instrument is editable and adaptable to allow updates to accommodate the addition of other cybersecurity standards. Given that the HCYMAF model was originally developed to evaluate higher education institutes (HEI) in the UK, it was adapted in this study to include the following standards relevant to Institutes of Higher Education (IHEs) in the United States: The Family Educational Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPPA), and the USG Cybersecurity policy.

The Maturity Model is a supplemental document that provides guidance on grading the HCYMAF. It has been updated to be inclusive of terminology and best practices that are relevant to the examined university in the United States. Accordingly, the following updates were applied: replacement of Higher Education Institute (HEI) with Institutes of Higher Education (IHE) to promote consistency with terminology used in the US, removal of GDPR, addition DoD, FERPA, HIPPA, GLBA and USG IT Handbook, and replacement of "international best practices" with "applicable international best practices".

The sections following offer insight into the relevance of each standard that was incorporated into the adapted version of the instrument.

FERPA

The Family Educational Rights and Privacy Act (FERPA) is a Federal law that protects the privacy of student education records. It applies to all schools that receive funding under an applicable program of the U.S. Department of Education.

HIPPA

The Health Insurance Portability and Accountability Act (HIPPA) applies to the healthcare industry and does not apply to college/university education records given that student records at campus health clinics are considered education records or treatment records under FERPA. However, HIPPA is considered in this study given the implications it has relevant to FERPA.

USG\Board of Regents Standards

According to the USG website, "the Georgia Constitution grants the Board of Regents the exclusive right to govern, control, and manage the University System of Georgia ("USG") and all USG institutions. The Board exercises and fulfills its constitutional obligations, in part, by promulgating rules and policies for the governance of the USG and its constituent units. The purpose of this Policy Manual is to collect, organize, publish, and otherwise make publicly available the directives and policies of the Board." The evaluated institution resides in the USG. Therefore, the corresponding standards were considered in this study.

The University System of Georgia (USG)\Board of Regents (BOR) policy standards are accessible online via the USG IT Handbook (University System of Georgia IT Handbook)

The USG Cybersecurity policy, which is included in the USG IT Handbook, encompasses the aforementioned FERPA and HIPPA standards. It also integrates the following related cybersecurity frameworks: The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and the NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management. And, it references the following cybersecurity policies and standards: the USG Business Procedures Manual, the GLBA "Safeguards Rule" , Critical Security Controls for Effective Cyber Defense v7.1, DoD Cybersecurity Maturity Model Certification v0.6, FERPA (PTAC): Data Security Checklist, DHHS Office for Civil Rights | HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework, 45 CFR 160, 162, and 164, Information Technology-Security Techniques Requirements, NIST SP 800-53 Rev4, Security and Privacy Controls, NIST SP 800-171 Rev. 1 Informative Reference Details, and Mapping Payment Card Industry Data Security Standard (PCI DSS) v3.2.1 to the NIST Cybersecurity Framework v1.1.

RESULTS

The Holistic Cybersecurity Maturity Assessment Model Framework (HCYMAF) is a very thorough, adaptable tool for conducting self-assessment of cybersecurity maturity in higher education institutes. The application of the tool in this study supported the organizations ability to evaluate and assess its current policies to support understanding of the overarching cybersecurity standards and promote enhancement of local policies.

Although SSU is in compliance with the USG policy standards and is appropriately applying cybersecurity measures in the organizational environment, in terms of maturity, this study revealed that there are opportunities for growth.

Thus, based on feedback received from the SSU ITS mentors, review of Savannah State's Security Policies, and application of the Revised Maturity Model, Savannah State's currently documented policies rank at the bottom level in terms of maturity as incomplete. The maturity levels of the model are shown in Figure 2 below, SSU is currently operating at Level 0:

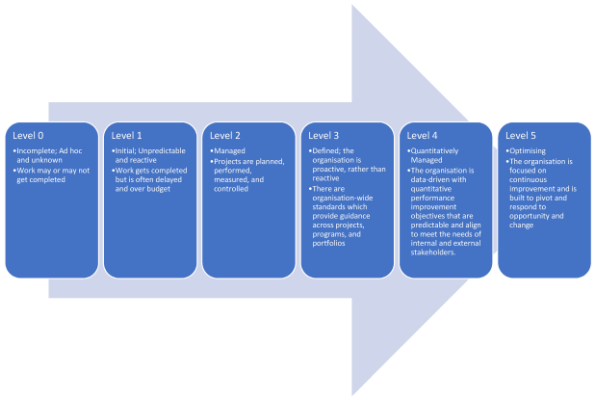

Figure 2. Maturity levels of the Holistic Cybersecurity Maturity Assessment Model

These results indicate that although some relevant work is being completed and security measures are being implemented and managed, the documented policies do not currently reflect the level of work that is being done. Therefore, SSU should consider taking action to ensure that the documented policies reflect the cybersecurity measures that are actually being applied and implement enhancements to the policies to promote higher levels of maturity.

RECOMMENDATIONS

To enhance its Cybersecurity Maturity, Savannah State University should take the following action:

- Ensure that policies are developed to align with each requirement of the NIST. Current policies do not address all aspect of the NIST.
- Incorporate more policies related to risk mitigation and response to attack. Current policies primarily focus on preventive measures to support cybersecurity.
- In instances where the university does not have a unique policy but is referencing a USG policy relevant to an area of the NIST, document a university policy that references the policy being employed. Current published policies do not consistently reference the USG policy.
- Consider a more centralized approach to cybersecurity that ensures that all responsible entities (i.e. Finance, IT, Plant Operations, etc.) work collaboratively to develop policies and ensure cybersecurity. Current cybersecurity policies and practices are managed across departmental functions.
- Develop a NIST Crosswalk to ensure that they have policies that are aligned with each aspect of the NIST and identify their alignment. Current published policies do not reference the NIST.
- Hire or designate dedicated administrative personnel that will be responsible for facilitating policy development and updates; ensuring policies are being implemented, managing mitigation efforts and incident response, maintaining records of incident and related responses, ensuring stakeholders are trained and managing policy updates on a specified rotational basis. There currently is not a dedicated Information Security Officer (ISO).
- Update the Quarterly Cybersecurity Program Review Questionnaire to not only assess the availability to resources and policies but also the extent of application and level of effectiveness. The current assessment questionnaire employed by the USG only evaluates the presence of cybersecurity resources and policies but does not evaluate application or effectiveness.

DISCUSSION

Although Savannah State University's cybersecurity policies are appropriately aligned with the expectations of the University System of Georgia (USG) Cybersecurity policies as outlined in the IT Handbook, much work is needed to support maturity. While the implementation of policies is a step towards enhanced levels of cyber hygiene (Cain, Edward, and Still, 2018; Maennel, Mäses, & Maennel 2018), additional work is needed to obtain the appropriate resources, further develop current policies to appropriately support mitigation of risks and responsiveness to attacks, implement a centralized cybersecurity approach, and employ assessment measures that promote cybersecurity maturity.

The University System of Georgia (USG) and Savannah State University are aware that the current policies need to be developed to support higher levels of cyber hygiene and maturity. Both are in the process of implementing enhancements to current cybersecurity best practices and policies. In doing so, they should consider the implications of the Holistic Cybersecurity Maturity Assessment Framework (HCYMAF) (Aliyu et al, 2020) and adopt the adapted version of the maturity assessment that has been employed in this study to further evaluate its cybersecurity and proposed future action toward promoting a more mature approach to cybersecurity that will foster a more secure environment that supports cyber awareness, implements policies and procedures that endorse cyber hygiene and demonstrates the responsiveness and adaptability necessary to stimulate future cyber maturity. Findings of this study will be shared with the appropriate SSU and USG IT personnel to support enhancement of current policies.

Future research should apply the HCYMAF to other higher education institutions in the US and abroad. Other adaptations of the instrument should also be explored for higher education institutions who are governed by alternative state and local standards.

REFERENCES

1. ALEXEI, A., & ALEXEI, A. (2021). Cyber Security Threat Analysis In Higher Education Institutions As A Result Of Distance Learning. International Journal of Scientific & Technology Research.
2. Aliyu, A., Maglaras, L., He, Y., Yevseyeva, I., Boiten, E., Cook, A., & Janicke, H. (2020). A holistic cybersecurity maturity assessment framework for higher education institutions in the United Kingdom. Applied Sciences, 10(10), 3660.
3. Cain, A. A., Edwards, M. E., & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. Journal of information security and applications, 42, 36-45.
4. Chapman, J. (2019). How Safe is Your Data?: Cyber-security in Higher Education. Higher Education Policy Institute.
5. Coghian, D. (2001). Insider action research projects: Implications for practicing managers. Management Learning, 32(1), 49-60.
6. Critical Security Controls for Effective Cyber Defense v7.1. Retrieved from: https://www.cisecurity.org
7. Cyber Security. Savannah State University. Retrieved from: https://www.savannahstate.edu/cyber-security/index.shtml
8. Cybersecurity. University System of Georgia. Retrieved from: https://www.usg.edu/cybersecurity

9. Cybersecurity Considerations for Institutions of Higher Education. Retrieved from: https://rems.ed.gov/docs/Cybersecurity_Considerations_for_Higher_ed_Fact_Sheet_508C.pdf
10. Data Security: K-12 and Higher Education. Retrieved from: https://studentprivacy.ed.gov/security
11. DHHS Office for Civil Rights | HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework, 45 CFR 160, 162, and 164. Retrieved from: https://www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rulecrosswalk-02-22-2016-final.pdf
12. DoD Cybersecurity Maturity Model Certification v0.6. Retrieved from: https://wwwcomplianceforge.com
13. Family Educational Rights and Privacy Act (FERPA). Retrieved from: https://studentprivacy.ed.gov/node/548/.
14. FERPA (PTAC): Data Security Checklist. Retrieved from: https://studentprivacy.ed.gov/resources/data-security-checklist
15. GLBA "Safeguards Rule". Retrieved from: https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reformproceedings/safeguards-rule
16. Health Insurance Portability and Accountability Act (HIPPA). Retrieved from: https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html and https://www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf.
17. Holistic Cybersecurity Maturity Assessment Framework (HCYMAF). Retrieved from: https://csma.somweb.gr/backend
18. Information Technology-Security Techniques Requirements. Retrieved from: https://www.iso.org/standards/54534.html
19. Kim, E., & Beuran, R. (2018, October). On designing a cybersecurity educational program for higher education. In Proceedings of the 10th International Conference on Education Technology and Computers (pp. 195-200).
20. Maennel, K., Mäses, S., & Maennel, O. (2018, November). Cyber Hygiene: The Big Picture. In Nordic Conference on Secure IT Systems (pp. 291-305). Springer, Cham.
21. Mapping Payment Card Industry Data Security Standard (PCI DSS) v3.2.1 to the NIST Cybersecurity Framework v1.1. Retrieved from: https://www.pcisecuritystandards.org/pdfs/Mapping-PCI-DSS-to-NISTFramework.pdf
22. National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). Retrieved from: https://www.nist.gov/cyberframework
23. NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management Retrieved from: https://nist.gov/privacy-framework.
24. NIST SP 800-53 Rev4, Security and Privacy Controls. Retrieved from: https://csrc.nist.gov/publications/sp800
25. NIST SP 800-171 Rev. 1 Informative Reference Details. Retrieved from: https://www.nist.gov/nist-sp-800-171-rev-1-informative-reference-details-ORhttps://www.nist.gov/document/csf-sp800-171mappingxlsx
26. Norris, D. F., Mateczun, L., Joshi, A., & Finin, T. (2019). Cyberattacks at the Grass Roots: American Local Governments and the Need for High Levels of Cybersecurity. Public Administration Review, 79(6), 895-904.
27. Othmana, Z., Rahimb, N., & Sadiqc, M. The Human Dimension as the Core Factor in Dealing with Cyberattacks in Higher Education.
28. Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations Retrieved from: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf
29. Savannah State University Contingency Plan. Retrieved from: https://www.usg.edu/cybersecurity/incident_reporting.
30. Savannah State University Policies & Procedures. Retrieved from:https://www.savannahstate.edu/cyber-security/security-policies.shtml.
31. Security Policies. Savannah State University. Retrieved from:https://www.savannahstate.edu/cyber-security/security-policies.shtml
32. Slonka, K. J. (2020). MANAGING CYBER SECURITY COMPLIANCE ACROSS BUSINESS SECTORS. Issues in Information Systems, 21(1).
33. Such, J. M., Ciholas, P., Rashid, A., Vidler, J., & Seabrook, T. (2019). Basic Cyber Hygiene: Does It Work?. Computer, 52(4), 21-31.
34. Technology Services Handbook, University System of Georgia. Retrieved from: https://www.usg.edu/information_technology_services/it_handbook/
35. Ulven, J. B., & Wangen, G. (2021). A Systematic Review of Cybersecurity Risks in Higher Education. Future Internet, 13(2), 39.
36. USG IT Handbook. Retrieved from: https://www.usg.edu/information_technology_services/it_handbook/ and https://www.usg.edu/information_technology_services/assets/information_technology_services/documents/ITHB_Crosswalk_Guide_v2.0.pdf.
37. University System of Georgia (USG) IT Handbook Cybersecurity. Retrieved from: https://www.usg.edu/cybersecurity/
38. Woody, C., & Creel, R. (2021). Lessons Learned in Building and Implementing an Effective Cybersecurity Strategy. Acquisition Research Program.
39. Zalaznick, M. (2013). Cyberattacks on the rise in higher education. University Business.