International Journal of Cybersecurity Intelligence & Cybercrime

Volume 3 | Issue 2 Article 4

11-3-2020

Proposal for the Development and Addition of a Cybersecurity Assessment Section into Technology Involving Global Public Health

This paper discusses and proposes the inclusion of a cyber or security risk assessment section during the course of public health initiatives involving the use of information and communication computer technology. Over the last decade, many public health research efforts have included information technologies such as Mobile Health (mHealth), Electronic Health (eHealth), Telehealth, and Digital Health to assist with unmet global development health needs. This paper provides a background on the lack of documentation on cybersecurity risks or vulnerability assessments in global public health areas. This study suggests existing frameworks and policies be adopted for public health. We also propose to incorporate a simple assessment toolbox and a research paper section intended to help minimize cybersecurity and information security risks for public, non-profit, and healthcare organizations.

cybersecurity, cyber risk management, frameworks, global public health, mHealth, digital health

Recommended Citation

Mierzwa, S., RamaRao, S., Yun, J. A., & Jeong, B. G. (2020). Proposal for the development and addition of a cybersecurity assessment section into technology involving global public health. International Journal of Cybersecurity Intelligence and Cybercrime, 3(2), 48-61. https://www.doi.org/10.52306/03020420BABW2272

IJCIC Center for Cybercrime Investigation & Cybersecurity

Proposal for the Development and Addition of a Cybersecurity Assessment Section into Technology Involving Global Public Health

Stanley Mierzwa*, Center for Cybersecurity, Department of Criminal Justice, Kean University, New Jersey, USA

Saumya RamaRao, Population Council, New York City, New York, USA

Jung Ah Yun, Department of Public Administration, Kean University, New Jersey, USA

Bok Gyo Jeong, Department of Public Administration, Kean University, New Jersey, USA

Keywords; cybersecurity, cyber risk management, frameworks, global public health, mHealth, digital health

Abstract:

This paper discusses and proposes the inclusion of a cyber or security risk assessment section during the course of public health initiatives involving the use of information and communication computer technology. Over the last decade, many public health research efforts have included information technologies such as Mobile Health (mHealth), Electronic Health (eHealth), Telehealth, and Digital Health to assist with unmet global development health needs. This paper provides a background on the lack of documentation on cybersecurity risks or vulnerability assessments in global public health areas. This study suggests existing frameworks and policies be adopted for public health. We also propose to incorporate a simple assessment toolbox and a research paper section intended to help minimize cybersecurity and information security risks for public, non-profit, and healthcare organizations.

Introduction

The increased use of technology solutions, whether hardware or software products, has greatly affected the field of global public health research, as well as the management of public, non-profit, and healthcare organizations for more than a decade. These technology solutions can help with innovative new approaches to reach consumers of healthcare, streamline data capture methods, automate mundane processes, and bring about speed efficiencies when tackling global public health challenges.

*Corresponding author

Stanley J. Mierzwa, M.S., Center for Cybersecurity, School of Criminal Justice, Kean University, 1000 Morris Avenue., Union, NJ, 07083, U.S.A.

Email: smierzwa@kean.edu

Many of these technology solutions have been labeled as mHealth, eHealth, Digital Health, and Telehealth products. These technology solutions rely on connected technologies using private and public networks such as the Internet. One of the main goals of introducing such technology is to empower individuals to manage and supplement their own health care and reduce costs for healthcare systems. The widespread growth in the use of mobile devices, such as smartphones, has contributed to the popularity and introduction of these technology solutions.

With increased use of technology solutions in existing organizations, cybersecurity has surfaced as an emerging issue facing society and organizations in all sectors. Computer security or cybersecurity is not new. One of the first known computer worms, called Creeper, was developed in 1971 by Bob Thomas. Revolutionary at that time, Creeper could move from computer to computer. The virus spread through the ARPANET (the precursor to the Internet) and displayed a message that said, "I'm the creeper, catch me if you can!" (Easttom, 2011). Although the Creeper virus did not cause any damage, many new and much more dangerous cybersecurity vectors have been developed that cause damage to information, systems, and products. Since then, computers have become more commonplace, accompanied by the growth of cyber threats. As such, the number of confirmed data breaches in the healthcare sector came in at 521 in 2020 versus 304 in 2019, an increase of approximately 42% (Verizon Data Breach Report, 2020). Cyberattacks cost healthcare organizations an average of approximately $1.4 million due to recovery fees and productivity lost (Fortified Health Security, 2020). An additional negative financial by-product of cybersecurity breaches involves costs to repair an organization's image because of attacks. Breached hospitals were associated with significantly higher advertising expenditures in the two years after the breach, yielding a 64% increase in annual advertising costs (Choi & Johnson, 2019). Furthermore, the growth of breaches to the healthcare sector by hacking has continued to increase from 12% in 2014 to 59% in 2019 (Fortified Health Security, 2020).

Despite the increased demand and use of technology solutions in health industries, scant literature has focused on the issue of cybersecurity risk assessments in the global public health field. This paper focuses on whether global public health practitioners and researchers perform or consider performing cybersecurity risk assessments in their digital health initiative projects, document their efforts, and include their results in research findings and resulting papers. We present the results of a literature review of journal articles found in PubMED Central, a free full-text archive of biomedical and life sciences articles and literature at the U.S. National Institutes of Health's National Library of Medicine, and conclude with proposing a cybersecurity toolkit to be deployed.

Literature Review

Background of Innovative Health Care Technology

Innovations in the use of mobile and electronic technologies in global public health research continue to gain momentum, as public, non-profit, and healthcare organizations incorporate these technologies as essential components in their operation and management systems. Part of this momentum is driven by the potential for profits; for example, interconnected health products are expected to be worth $285 billion by 2022 (Alvarenga & Tanev, 2017; Harris, 2014). Many new concepts for mHealth/eHealth/Telehealth will be piloted by health care implementers and researched by health care providers in the private, public, and non-profit sectors.

The deployment of innovations typically starts as a pilot before going to scale. It is important to build in tasks associated with minimizing cyber risks from the beginning of the pilot phase.

The United Nations Sustainable Development Goal (SDG) 3 aims to ensure healthy lives and promote wellbeing for all. Ample digital health innovations aim to contribute to SDG 3. Specifically, SDG 3 states good health and wellbeing direct patient interaction, and thus health informatics and telemedicine can be improved through better connectivity. In 2017, the International Telecommunication Union (ITU), a specialized agency of the United Nations responsible for issues and concerns related to information and communications technology, launched "Digital Health for Africa." This is a partnership to scale up the use of digital technologies to strengthen the delivery of public health services in Africa. Another such effort is "Be He@lthy, Be Mobile," a collaboration between ITU and the World Health Organization (WHO) that assists governments in introducing and scaling up digital mHealth services (International Telecommunications Union, 2017).

Increased Innovations and Need for Cybersecurity Risk Assessments

As technology health products and innovative digital solutions continue to increase, researchers and information technology engineers must always consider the risks associated with their technology implementations. Given the hyper-sensitivity and attention assumed to cybersecurity in this current day and climate, it would be negligent not to provide such a focus (Mierzwa et al., 2019). Risk assessments are valuable in determining whether conditions may bring about greater threats that could result in problems for end-users, investigators, and system managers.

The most fundamental goal of a cybersecurity risk assessment is to understand the risk to an organization or research project in the context of mission, operation and functions, human safety, reputation, and assets.

At its most vital core, the reason for performing a cybersecurity risk assessment is to identify gaps where potential threats and vulnerabilities can be introduced and damage the developed system, or the information stored and/or processed. A vulnerable digital health system can compromise patient data, expose patients to potential discrimination and/or stigma, and bring about reputational harm to the health provider. Furthermore, addressing a threat after it has been unleashed and then mitigating the effects increase costs to the health system.

Cybersecurity issues surrounding technology continue to grow, and the demand for cybersecurity professionals is rising. In fact, the Bureau of Labor Statistics, U.S. Department of Labor Occupational Outlook Handbook states that job growth for Information Security Analysts is expected to be 32% between 2018 and 2028. This projected growth is compared to a predicted 5% increase for all other occupations (Bureau of Labor Statistics, 2018).

There are other positive by-products of conducting risk assessments. One is that the process of conducting a risk assessment will bring increased and heightened awareness of the implementers of the digital health initiative. Many fields and disciplines are still learning about cybersecurity issues, and this is also true for public health policymakers, program designers, and researchers. Cybersecurity or risk assessments are not as prevalent in global public health research discussions of mHealth/eHealth/Telehealth/Digital Health. It might be because cybersecurity is not part of the general public health curriculum.

Alternatively, Computer Science and Information Technology disciplines include such guidance. For example, Information Assurance and Security has been added as a core topic in the ACM/IEEE Computer Science Curriculum and IT curriculum.

There are also continuing efforts to promote cybersecurity education to K-12 teachers and students (Cai, 2018).

Another beneficial by-product of cybersecurity risk assessment involves improving the way a health implementation and research team communicate about cybersecurity in general. For example, many research protocols and papers include "Discussion" and "Methods" sections; however, cybersecurity has yet been the focus as an independent section or as one of the main themes in existing sections in research surrounding Digital Health efforts.

Safety and Security

When considering the reasons to be concerned about cybersecurity in global public health service delivery and research, one needs to focus on people's physical safety and security. Public health research projects often include the use of subjects – people; because of this, a premium must be placed on security to ensure the safety of research study participants. In HIV research trials, for example, these data security practices are even more critical as breaches of confidentiality may negatively impact participants' lives (Andriesen, et al., 2017).

Existing US-Based Legislation

For eProducts utilized in healthcare-related settings, government and industry regulations impose certain guidelines. The two dominant pieces of legislation that affect the security parameter of digital health apps are the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act, referred to as the HITECH Act (Garrie & Paustian, 2014). These laws include the protection of electronic information and attention to cybersecurity. However, for many mHealth/eHealth or Telehealth projects that include an introductory or "pilot" phase, these regulations may not be applied because the project is in the inception stage and there may not be sufficient resources available to pursue compliance; thus, the potential to increase cybersecurity risk might not be addressed from the outset.

Relatedly, the Federal Policy for the Protection of Human Subjects, also known as the Common Rule of 1991, governs the conduct of human subject research. The Common Rule has antecedents in the Belmont Report of 1979, where the principles of respect, beneficence, and justice were articulated to protect human subjects from harm emanating from their participation in health research (RamaRao et al., 2007). The Common Rule policies and guidelines for IRBs, informed consent, and Assurance of Compliance provide guidance on how adverse events are to be reported, handling sensitive data including biological data, and protection for exposed biological data among vulnerable populations (Agora et al., 2014).

By highlighting the principles of privacy, confidentiality, respect, protection from harm, and justice, these legislations require digital health implementers to ensure that these principles are included in the design and deployment of their interventions.

Existing NIST Cybersecurity Framework (CSF)

The popular National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) is a tool for employing the best practice in assessing risks to computer security in an organization.

The NIST framework is very comprehensive and often utilized by staff with an Information Technology background.

It is organized into five functions:1) Identify 2) Protect 3) Detect 4) Respond and 5) Recover.

The NIST framework is very comprehensive and often utilized by staff with an Information Technology background. It is organized into five functions:1) Identify 2) Protect 3) Detect 4) Respond and 5) Recover. Within each function, there are categories and subcategories to be analyzed; these could be specific guidelines to access control, software updates for vulnerabilities, and endpoint protection. Finally, there are tiers of implementation to demonstrate maturity: Tier 1 through Tier 4. The higher tiers demonstrate the highest level of adoption. By way of history, the original NIST Cybersecurity Framework was born out of U.S. President Barack Obama's signing of Executive Order 13636 in 2013 – this paved the way for a common language and a set of standards for improving cybersecurity. The most recent version of the CSF (Version 1.1) was released in 2018. In May 2017, U.S. President Donald Trump signed Executive Order 13800, making government agency heads accountable to the President for implementing the NIST Cybersecurity Framework. In this Order, each agency head is to provide a risk management report to the Secretary of Homeland Security and the Director of the Office of Management and Budget (The White House, 2017).

The NIST CSF is extensive and approaches an entire organization, and thus may be too daunting for implementers and research investigators embarking on digital health projects. The NIST CSF is geared towards critical infrastructure. However, it does have many best practices that should be reviewed by those introducing technology. In the next section, we propose a framework that draws upon the essential elements of the NIST CSF so that digital health implementers can feasibly introduce cybersecurity risk assessments in their initiatives and interventions.

Methods

Literature Search

A systematic search was conducted for cybersecurity risk assessments published between 2000 and 2019. Key search terms were derived from a review of the literature and included terms such as "cybersecurity risk assessment", "computer security," and "digital health." An advanced search in the online U.S. National Library of Medicine, National Institutes of Health PubMED database, scanning for all articles via a full-text search, yielded over 59,000 articles. We then performed more focused searches using the PubMED Advanced Search Builder function; the results can be seen in Figure 1. We iteratively refined the search criteria by making it more specific. This refinement resulted in 14 relevant articles relating to digital health and cybersecurity. Given the nature and expansion of digital health, which includes components of connected technology components, such a small number of articles demonstrates the lack of attention being given to cybersecurity and the associated risk assessments.

We performed an additional search using the PubMED MeSH (Medical Subject Headings) controlled vocabulary, which is used to index all articles found in the PubMED database. Articles can be cataloged using multiple MeSH headings. Since there is no specific MeSH index for "Cybersecurity" specifically, we used "Computer Security."

Of the 14 articles we found to be relevant, we focused on the contents of the freely available resources; this reduced the number to seven articles, which were further evaluated. Two specific articles from the review bring up the fact that additional research and measures are needed to effectively minimize risk to privacy and security in mHealth. Shifali et al. (2014) provide a table of common cybersecurity risks and cost-effective solutions that can be implemented with research efforts into Internet/eHealth and telemedicine.

Wethington et al. (2019) produced research recommendations from a workshop related to mHealth technologies. The results of the 2019 mHealth workshop produced two categories of recommended and expanding research on mHealth cybersecurity and privacy issues that have received attention in the area of implementation into practice and regulatory issues.

In summary, our literature search in PubMED indicated that there is a gap in or lack of formal documentation regarding the performance of cybersecurity risk assessments, specifically in the realm of producing research on public health.

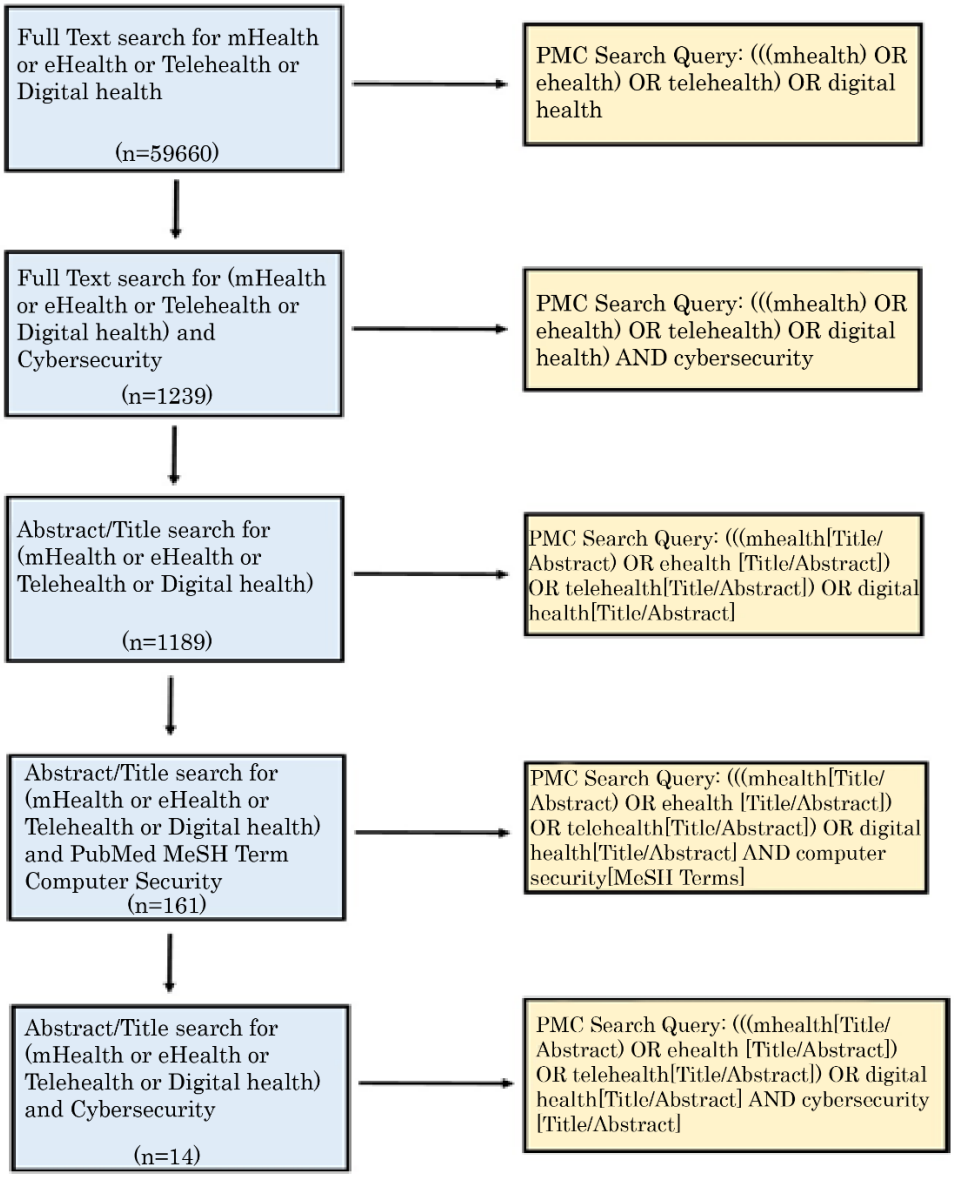

Figure 1. PubMED Focused Search Results – Criteria and Query String as of 12/2/201

Proposed Cybersecurity Risk Assessment Framework

Proposed Theoretical Model Design Concept Cybersecurity Framework

There exists an abundant array of different frameworks related to information security and cybersecurity. Many of these frameworks may be aligned and created for particular industry sectors, such as banking, handling of credit card data, and infrastructure utilities, such as electricity.

In considering the seven phases of the Software Development Life Cycle (SDLC), one can introduce the idea of a cybersecurity risk assessment in any of the following phases: System Planning, System, Requirements, Design, Development, Testing, Deployment, and Maintenance.

Global public health efforts that include a technology component can focus on any of several phases in the SDLC. For example, digital health implementation or research can focus on the concept or innovation phase, or on how a team may wish to build or release a product to the field. Regardless of which area will be researched and explored, it is possible to do a specific cybersecurity risk or threat analysis in any SDLC phase, as demonstrated in Figure 2 below.

We propose a roadmap for including risk assessments in the lifecycle of a digital health intervention. Figure 2 shows that risk can be evaluated at or during any of the phases, which encompass the bulk of categories relevant during the creation of digital health technology.

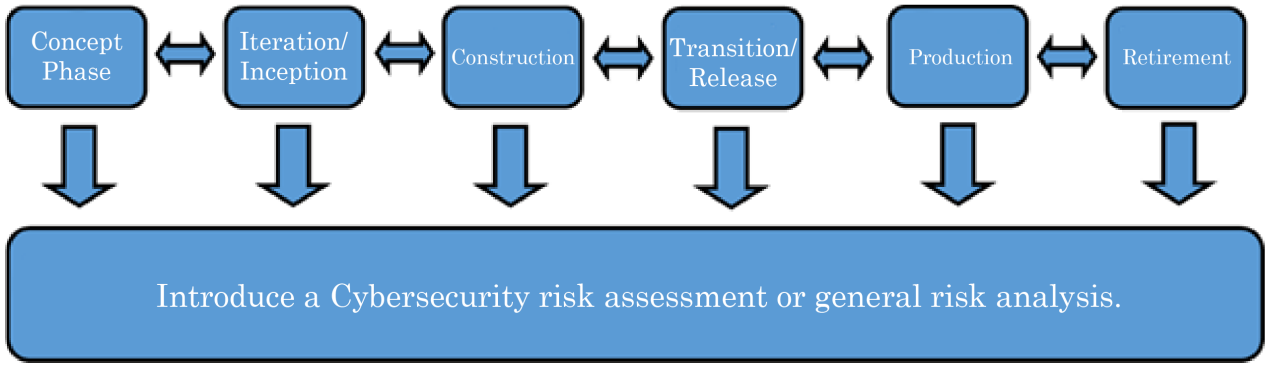

Figure 2. Technology Development Lifecycle Phases with Cybersecurity Risk Analysis.

Many pilot-related global health public research efforts would involve going through all the phases, such as in the development of a mobile software application, or App, or hardware device. In this case, researchers would benefit from doing a risk or threat assessment in the respective phases documented in the proposal.

Cybersecurity Checklist

Components in the NIST CSF will be utilized as a starting block to introduce digital health implementers and researchers to the five main core functions—Identify, Protect, Detect, Respond, and Recover. The NIST CSF is divided into three key parts: "Core," "Profile" and "Tiers." Each of the functions is subdivided into a total of 23 categories.

For each category, there are a number of subcategories of security controls and outcomes, totaling 108 subcategories in all. In the interest of a simplified approach, and to bring light to being proactive and placing emphasis on risk analysis, the authors propose considering the first two functions within the "Core" part. The Identify and Protect functions are crucial to bringing awareness to cybersecurity threats that the public health researchers may not be familiar with. These two functions go a long way to advancing education surrounding best practices in cybersecurity or cyber-hygiene. The Detect, Respond and Recover functions are equally important, but the authors feel that these activities would be best approached by the organization's Information Technology or Security teams and departments, who are more familiar with and trained in the activities involved in these three last functions.

General Cybersecurity Risk Assessment Guidelines

The inclusion of cybersecurity awareness in the form of a discussion or project task as the first step for public health implementers and researchers involved in technology is a positive step towards minimizing threats and vulnerabilities. With public health initiatives, there is usually a team leader. This individual is the overall project manager providing technical and managerial oversight. Bringing project managers into discussions about cybersecurity will impress upon them the importance of including tasks utilizing resources to help perform assessments.

Global Public Health Research Technology Cybersecurity Framework (GPHR-TCF)

As a more progressive effort, we have outlined a general workflow that one can follow step-by-step to perform a cybersecurity risk analysis. In Figure 3, we outline an approach and workflow one can use to perform a specific cybersecurity risk analysis, or self-assessment, within a digital health project. The workflow permits doing as many risk analysis scenarios as required and offers flexibility based on the technology architecture created.

The workflow diagram of the seven sets of blocks depicted in Figure 3 includes the following steps:

1. Select a phase from within the technology development lifecycle, described in Figure 2 that is being addressed.
2. Discuss and introduce the concept of a cybersecurity risk assessment.
3. Determine which part of the two NIST functions (Identify or Protect) to pursue.
4. Depending on the specific technology used, created, or researched, select the NIST Identify (blue) or Protect (purple) functions an area from the group to assess. For reference, the cybersecurity Framework Function and Category Unique Identifiers are seen in Table 1.
5. Note the top three cyber threats or concerns related to either a remote or local attack surface. In considering the attack surface, the remote surface could be a system or solution available via the public Internet, or requiring connection to a private network; the local surface could be a smartphone, tablet, or laptop device.
6. Rank the three threats into a Likelihood/Consequence grid.

7. Determine, based on the technology solution analyzed, what, if any, modifications should be made to minimize the threats.

Table 1. *NIST Cybersecurity Function and Category Unique Identifiers – Source NIST Cybersecurity Framework 1.1*

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

If applicable, return to the top of the workflow and repeat for the next potential lifecycle phase to be analyzed.

This workflow outline may seem obvious, but it does force one to do an analysis and, more importantly, to document the results. These results could be made available in a research paper if pursued in the course of the research project.

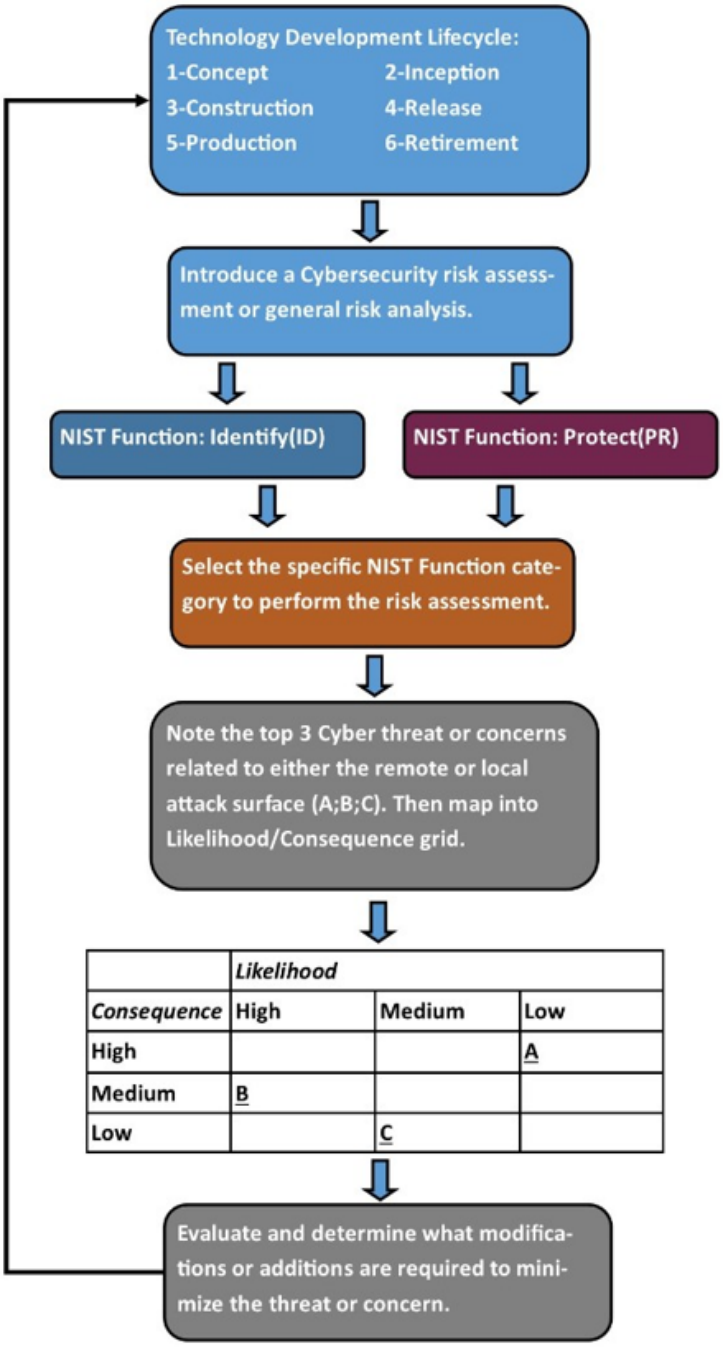

Figure 3. Cybersecurity Risk Analysis Workflow

The authors have named the referenced proposed concept 'Global Public Health Research Technology Cybersecurity Framework (GPHR-TCF).'

Discussion

In performing the PubMED literature search, 14 articles related to digital health platforms and cybersecurity were found, which seemed surprisingly low. Further exploring the global public health curriculum for the inclusion of cybersecurity topics may be warranted. A possible area for more detailed research includes cybersecurity coursework in the myriad of graduate programs that may be producing digital health solutions as part of the coursework or curriculum of these programs. Additionally, consideration of the benefits of a campaign can be considered for those who work in the global public health sphere where technology is a must. For reference, the national public awareness campaign "STOP.THINK.CONNECT" raised consciousness about cyber threats. Perhaps a similar, more modest campaign can be envisioned for the implementation to the research community.

It should be considered to embrace cybersecurity as a core theme in future research papers with a technology component. The benefits of using technology and web-connected products are well known in global public health areas. Introducing, at a minimum, a cyber-risk likelihood and consequence analysis would bring confidence to those facilities in public, non-profit, and health-service organizations that utilize the proposed technology solution (Mierzwa et al., 2019). These assessments are meant to be proactive regarding threats and, to some degree, should lessen the extent of having to react to being hacked or having vulnerabilities exploited.

The authors would also like to bring our attention to other areas in the global public health technology sector that warrant a focused examination of cybersecurity – such as the Open Data initiatives or the Common Data Models. These initiatives and programs, currently being developed and pursued, invite contributions from the industry and academia.

An emerging technology for validating and protecting transactional data is Blockchain. In the interest of protecting the confidentiality, integrity, and availability of private information used in the course of digital health research projects, Blockchain can be leveraged as an idea for future research. Blockchain may help secure the integrity of an entire, overall digital health solution.

Finally, as a follow-up to the current study, an effort is being pursued as part of a faculty seed grant application. A team of faculty and practitioners in Computer Science, Public Administration, and Criminal Justice will conduct research partnering with their undergraduate and graduate students to further evaluate the awareness and preparedness of cybersecurity in nonprofit global health service organizations. By this inter-disciplinary collaboration, at the intersection of cybersecurity and non-profit health administration, this research will contribute to developing cybersecurity materials and a manual that could be used during the unprecedented COVID-19 health crisis.

Limitations

The authors highlighted knowledge about existing cybersecurity frameworks that are available but focused on discussing the NIST CSF as a core. This paper did not go into a detailed comparison of frameworks. Other such frameworks include the International Organization for Standardizations (ISO 27001/27001), the Payment Card Industry Data Security Standard (PCI DSS), and the Center for Internet Security (CIS Critical Security Controls).

The literature search focused on the use of the available online NIH PubMED database, which has an excellent search mechanism. There are many journals that could have been considered for review but might not have been included in the US NIH PubMED system.

Although this paper proposes the concept of a customized public health cybersecurity framework, an actual test, either theoretical or practical, did not take place. A potential next step would include applying the proposed framework and workflow to a public health research project that includes technology components found in such projects.

Conclusion

This paper brings forward a call to action for global public health implementers and researchers to include risk and vulnerability analysis during projects involving technology development and implementation. The initial concept of incorporating a consistent cybersecurity section in research papers containing a technology component was envisioned in a Chatbot feasibility, but this current paper pushes the idea a bit further (Mierzwa et al., 2019). The authors recognize that much more work is required to further the proposed concept of a customized workflow and framework that public health practitioners can utilize. The proposal to develop a framework and cybersecurity assessment workflow is a critical first step in addressing the growing cybersecurity risks associated with technology implementations in public health research, including a developed technology component.

Although the authors discuss the development of a focused cybersecurity workflow framework for use in public health research, such a tool could be developed or modified to be used by other fields with expanded use of technology tools, such as law enforcement and criminal justice.

For the literature review, the authors utilized the National Library of Medicine Medical Subject Headings (MeSH) that hierarchically organized vocabulary used for indexing and cataloging health-related data. Although “Computer Security” was included as a MeSH term, the authors request that the specific term “cybersecurity” be added to the Medical Subject Headings vocabulary to help bring further attention to this important topic.

The authors would like to propose further research and exploration into the area of cybersecurity education and awareness in the context of global public health research that includes a technology component. Evidence found in this paper suggests clarifying computer security benefits by further discovering the reasons for the limited literature. Our endeavors also include a step to validate the use of the suggested framework by implementing it in the next digital health project we embark on.

Acknowledgments

This research was supported by the Kean University Center for Cybersecurity, a multidisciplinary collaboration between the School of Criminal Justice and Public Administration and School of Computer Science and Technology. A special thank you to Dr. James Drylie for his support and vision of this collaborative team and to Netania Budofsky for her thorough edit and review of this research paper, she was instrumental and helpful in pointing out areas for improvements.

Declaration of Interest Statement

The authors declare that they have no conflicts of interest.

References

Agora, S., Yttri, J., & Nilsen, W. (2014). Privacy and security in mobile health (mHealth) research. *Alcohol Research, 36(1), 143-151.*

Alvarenga, A., & Tanev, G. (2017). A cybersecurity risk assessment framework that integrates value-sensitive design. *Technology Innovation Management Review, 7(4), 32-43.*

Andriesen, J., Bull, S., Dietrich, J., Haberer J. E., Van Der Pol, B., Voronin, Y., … & Priddy, F. (2017). Using digital technologies in clinical hiy research: Real-world applications and considerations For future work. *Journal of medical Internet research, 19*(7), e274.

Bureau of Labor Statistics. (2018). Occupational Outlook Handbook. Retrieved from https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

Cai, Y. (2018). Using case studies to teach cybersecurity courses. *Journal of Cybersecurity Education, Research and Practice, 2018*(2), 1-24.

Choi, S. J., & Johnson, M. E. (2019). Understanding the relationship between data breaches and hospital advertising expenditures. *The American journal of managed care*, *25*(1), e14-e20.

Easttom, C. (2019). *Computer Security Fundamentals (4h ed.).* Indianapolis, IN: Pearson IT Certification.

Fortified Health Security. (2020). Horizon Report The State of Cybersecurity in Healthcare. Retrieved from https://go.fortifiedhealthsecurity.com/2020-Horizon-Report-1.html

Garrie, R. & Paustian, P. (2014). mHealth regulation, legislation, and cybersecurity. In D. Malvey & D. J. Slovensky (Ed.), *mHealth.* (pp. 45-63). Boston, MA: Springer.

Springer, (pp. 45-63). Boston, MA.

Harris, P. (2014). The prognosis for healthcare payers and providers: Rising cybersecurity risks and costs. PricewaterhouseCoopers.

International Telecommunications Union. (2019). ICTs to achieve the United Nations Sustainable Development Goals. Retrieved from https://www.itu.int/en/mediacentre/backgrounders/Pages/icts-to-achieve-the-united-nations-sustainable-development-goals.aspx

Mierzwa, S., Souidi, S., Conroy, T., Abusyed, M, Watarai, H., & Allen, T.(2019). On the potential, feasibility, and effectiveness of chat bots in public health research going forward. *Online Journal of Public Health Informatics, 11*(2), e4

National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity. Retrieved from ttps://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

RamaRao, S., Friedland, B., & Townsend, J. W. (2007). A question of ethics: Research and practice in reproductive health. *Studies in Family Planning, 38(*4), 229-241.

Shifali, A., Yttri, J., & Nilsen, W. (2014). Privacy and security in mobile health (mHealth) research. *Alcohol Research Current Reviews*, *36*(1), 143-151.

Verizon Data Breach Report. (2019). Retrieved from https://enterprise.verizon.com/resources/executivebriefs/2020-dbir-executive-brief.pdf

Wethington, E., Eccleston, C., & Gay, G., Gooberman-Hill, R., Schofield, P., Bacon, E., … & Kenien, C. (2018). Establishing a research agenda on mobile health technologies and later-life pain using an evident-based consensus workshop approach. *The Journal of Pain*, *19*(12), 1416-1423.

Whitehouse.gov. (2017). Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. Retrieved from https://www.whitehouse.gov/presidential-actions/presidential-executive-order- strengthening-cybersecurity-federal-networks-critical-infrastructure/