CYBERSECURITY PEDAGOGY & PRACTICE JOURNAL

Volume 3, No. 2
October 2024
ISSN: 2832-1006

In this issue:

iscap
Information Systems & Computing Academic Professionals

The **Cybersecurity Pedagogy and Practice Journal** (**CPPJ**) is a double-blind peer-reviewed academic journal published by **ISCAP** (Information Systems and Computing Academic Professionals). Publishing frequency is two times per year. The first year of publication was 2022.

CPPJ is published online (https://cppj.info). Our sister publication, the proceedings of the ISCAP Conference (https://proc.iscap.info) features all papers, panels, workshops, and presentations from the conference.

The journal acceptance review process involves a minimum of three double-blind peer reviews, where both the reviewer is not aware of the identities of the authors and the authors are not aware of the identities of the reviewers. The initial reviews happen before the ISCAP conference. At that point, papers are divided into award papers (top 15%), and other accepted proceedings papers. The other accepted proceedings papers are subjected to a second round of blind peer review to establish whether they will be accepted to the journal or not. Those papers that are deemed of sufficient quality are accepted for publication in the CPPJ journal.

While the primary path to journal publication is through the ISCAP conference, CPPJ does accept direct submissions at https://iscap.us/papers. Direct submissions are subjected to a double-blind peer review process, where reviewers do not know the names and affiliations of paper authors, and paper authors do not know the names and affiliations of reviewers. All submissions (articles, teaching tips, and teaching cases & notes) to the journal will be refereed by a rigorous evaluation process involving at least three blind reviews by qualified academic, industrial, or governmental computing professionals. Submissions will be judged not only on the suitability of the content but also on the readability and clarity of the prose.

Currently, the acceptance rate for the journal is under 35%.

Questions should be addressed to the editor at editorcppj@iscap.us or the publisher at publisher@iscap.us. Special thanks to members of ISCAP who perform the editorial and review processes for CPPJ.

CYBERSECURITY PEDAGOGY AND PRACTICE JOURNAL

Editors

2024 Review Board

Feasibility of Creating a Non-Profit and Non-Governmental Organization Cybersecurity Incident Dataset Repository Using OSINT

Stanley J. Mierzwa
smierzwa@kean.edu

Iassen Christov
hristovj@kean.edu

Center for Cybersecurity
Kean University
Union, New Jersey 07083, USA

Abstract

Organizations of all types are prone to cybersecurity and information security attacks. Non-Profit Organizations (NPOs) and Non-Governmental Organizations (NGOs) are not exempt from using information technology solutions and, thus, have been the recipient victims of cyber attackers. There exist many areas and venues where data are collected to report back annually on the status and numbers of cybersecurity attacks against many sectors of our society. The Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) catalogs sixteen critical sectors that are considered vital to the United States. However, finding where the NPO and NGO community should reside with regard to a categorized sector is challenging. The cybersecurity incident data collected by many agencies does place a focus on the sixteen sectors. This effort and write-up will focus on the NPO and NGO communities and provide the process followed to create the data repository, categorization of attacks taxonomy, fields captured, outlets, and areas where data that is relevant to historical cybersecurity incidents in these types of agencies is available. In addition, the beginning of a running log and dataset for the NPO and NGO community will emerge to determine if this activity is feasible and can continue. A desired outcome for this effort is to make available a dataset that can be referenced by researchers, students, and leaders investigating cybersecurity risk management and analysis of the NPO and NGO sectors. In addition, this effort was started with the purpose of providing students from varied academic disciplines the opportunity to engage in practical pedagogical cybersecurity and cybercrime activity.

Keywords: Pedagogy; Cyber-attacks; Cybersecurity; Cybercrime; Non-Profit; Non-Governmental Organization

Recommended Citation: Mierzwa, S., Christov, I., (2024). Feasibility of Creating a Non-Profit and Non-Governmental Organization Cybersecurity Incident Dataset Repository Using OSINT . *Cybersecurity Pedagogy and Practice Journal;* v3 (n2) pp 48-57. https://doi.org/10.62273/EUFO3601

Feasibility of Creating a Non-Profit and Non-Governmental Organization Cybersecurity Incident Dataset Repository Using OSINT

Stanley Mierzwa and Iassen Christov

1. INTRODUCTION

There exists an unmet need or gap with regard to cybersecurity and cybercrime incident historical data from attacks against the non-profit and non-governmental organization arenas or communities. The role of sharing data is instrumental in cybersecurity research and will benefit organizations aiming to predict and protect against malicious attacks (Kouper & Stone, 2024). Understanding that organizations may opt not to disclose if and when a cyber-attack strikes them, open source avenues still exist where relevant information related to such breaches and attacks against the NPO and NGO sectors has been made available in the public domain. The Non-Profit Cyber Incident Repository (NPCIR), created as part of this activity, partnering with students, faculty, and staff, allows individuals the opportunity to study, refer, and distill a variety of data point insights related to cybersecurity attacks. The qualities or data elements provided include the country or region of the affected NPO or NGO, the general type of attack, the type of industry-focus organization, relation to the Confidentiality-Integrity-Availability (CIA) triad, the year of the attack, and many other fields.

Having historical data on previous cybersecurity attacks against NPOs and NGOs can be a valuable asset that can be referred to by critical stakeholders in these organizations so that they can better prepare to defend against upcoming attacks. Additionally, understanding the landscape of what types, frequency, and other critical cyber-attack qualities are utilized against these outfits may be helpful for NPOs and NGOs that wish to place greater emphasis and obtain approval to align more significant cybersecurity resources.

2. THEORETICAL MODEL AND FRAMEWORK

To guide the effort to envision, initiate, build, and pursue this novel research activity, the use of Open Source Theory was followed as a framework. The theory was introduced as a form of human behavior, generating the capabilities and potential for sharing information early and frequently, given the fast emergence and phenomenon of the Internet (Glassman, 2013). Key pillars followed by this relatively new theory include the development of new concepts, using tools commonly available to the masses, creation through practice, co-development of ideas, and focusing on a problem to solve (Glassman, 2013). Other studies have included the Open Source Theory in practice, including an investigation of this evolving framework (Choi & Glassman, 2017; Kim et al., 2015; Kuznetcova & Glassman, 2018).

3. LITERATURE REVIEW

Non-Profit and Non-Governmental Organizations

Understanding what constitutes a non-profit or non-governmental organization requires a brief definition. Although there may not be one wholly agreed-upon set of definitions, in considering the operation of a non-profit organization, it will consist of five essential characteristics, including being institutionalized as an organization, existing privately and separate from government, not returning any profits and being non-profit distributing, being of a self-governed model and configured with its internal governance, and in some degree allow for voluntary participation (Morris, 2000; Salamon & Anheier, 1992). Non-profits are more prone to not having ample budgets and resources to help safeguard their information technology and systems assets. They are considered a primary concern for their leadership and critical stakeholders (Ermicioi & Liu, 2022).

Non-Governmental Organizations can be involved in a variety of missions or focus activities. For one example, the role of NGOs has been formidable in the development and delivery of vaccines and vaccine development (Walton, 2017). Historically, the nomenclature or non-governmental organization term generally took shape during the time of the emergence of the United Nations, during the mid-1940s (Willetts, 2002). Many different mission-focused and variably structured NGOs exist in different parts of the globe and of varying sizes. This global landscape can introduce unique cyber challenges. As a form, the organization should be

independent of government management or control, without the aim to challenge governments as a political party, not for profit, and noncriminal (Willetts, 2002).

Existing Cybersecurity Incident Datasets

Known cybersecurity incidents have continued to rise substantially in organizations of many types, and this may only be tipping the case since not all breaches may be reported. Related to the NPO and NGO communities, an estimated 80% of nation-state attacks were directed against the broad swath of think tanks, government agencies, and NGOs (Lambert, 2021; Sobers, 2024). Over time, many different publicly accessible and available reports and datasets have emerged and, in some cases, continue to be routinely updated – meaning, it is not just a point-in-time snapshot of cyber incident attack information. The Critical Infrastructure Ransomware Attacks (CIRA) dataset and repository include records of attacks that are categorized as ransomware, and this information collection was initiated in 2019 (Rege, 2023). As of the time of this research, the CIRA database contains 1,654 ransomware attacks (Rege, 2023).

One other very broad-based, interactive, searchable cybersecurity event database is the CISSM Cyber Attacks Database, which is routinely updated (Harry & Gallagher, 2018). The solution permits quickly searching cyber-attack information with category types of actor type, attack type, and location. Another specific resource made available by the CommunityIT Innovators (2023) which is a non-profit organization that provides technology expertise to the NPO community. The resource provides a yearly snapshot view of NPO cybersecurity incident information within their client base (2023 Community IT Nonprofit Incident Report, 2023).

The United States Federal Bureau of Investigation (FBI) makes available and routinely provides reports via its Internet Crime Complaint Center (IC3 - Internet Crime Complaint Center, 2022). The IC3 is seen as the nation's central hub for providing the ability to report cybercrimes and review historically collected data via the availability of an annual report. The IC3 system does not provide the details and data to perform a deep dive into providing individual company or organization names. However, it does report on the ranking of the most frequent attack types and trends, along with an overarching landscape view of the previous year's internet breaches and cybercrimes reported into their portal.

Cybersecurity Focus on the NPO and NGO Environment

Relevant and excellent resources exist to aid the NPO and NGO sectors with activities, tasks, and methods to prevent cybersecurity attacks. Specific to the global public health NPO and NGO environments, Mierzwa et al. (2020) outlined ways these sectors could integrate strategies to minimize cyber risks. An abundance of cybersecurity frameworks exists in both the public domain and private (requiring purchase of subscription) domains. For some small businesses, which smaller or start-up NPOs may be categorized, the use of the freely available public domain genre of frameworks can be evaluated (Mierzwa & Klepacka, 2023).

Lack of Cybersecurity Incident Reporting Requirements on the NPO and NGO Community

In 2022, President Biden of the United States signed into law an act named the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). The act requires that organizations considered to be covered entities report to the United States Cybersecurity and Infrastructure Security Agency (CISA) when cybersecurity incidents or ransomware payments are made (CISA.GOV, 2022a). CISA is tasked with developing and issuing the regulations, which are expected to require covered entities to report cyber incidents within 72 hours from the time a cybersecurity incident occurs (CISA.GOV, 2022b). The development of CIRCIA is yet another notice requiring agencies and organizations to report cybersecurity incidents of notice potential. Thus, this research on the subject will further contribute to the knowledge and information available on this topic. In its annual Data Breach Investigations Report, Verizon states that incident reporting can be influenced by factors such as reporting laws and partner visibility, and some industries, such as entertainment or construction, may have low numbers reported because of a lack of requirements (Verizon, 2022). However, the sectors of NPOs and NGOs may not necessarily sit within any of the known entities and, as such, may not be required to report cyber-incidents.

Recent bipartisan legislation has emerged during 2022 that mandates the reporting of cyber incidents for specific critical infrastructure sectors of our nation, and the Cybersecurity and Infrastructure Security Agency (CISA) has been provided the opportunity to document the rule mechanics (Friedman & Mitchell, 2022). The importance of reporting can include many factors, but one essential product is to permit the timely

sharing of cyber threat activities that can benefit our critical infrastructure sectors.

Specific sectors, such as healthcare, are certainly affected by cyber-attacks but are widely under-reported. Specific reasons many health-related organizations under-report cyber incidents include not knowing what to report and how to do so (Cyber Peace Institute, 2021). This is despite an increase in such attacks as ransomware, which has doubled between 2016 and 2021, creating disruptions or inability to use healthcare systems and even canceling scheduled care (Neprash et al., 2022). Even if considered to be possibly underestimated, the Neprash et al. (2022) study also found that one in five ransomware attacks were not reported or available in the US Department of Health and Human Services Office of Civil Rights (HHS OCR) Data Breach Portal (Neprash & Rozenshtein, 2023).

4. METHODS

Data Collection for Repository

The ability to gain deeper knowledge and insight on a topic has become more accessible than ever and with incredible speed with the use of openly and freely available resources and information as a result of the growth of the Internet, specifically within the World Wide Web. Some of the earliest forms of essential Open Source Intelligence (OSINT) can be attributed to the Second World War, with the advent of investigations of free and available data and information and connecting with findings to incorporate actions (Glassman & Kang, 2012; Schaurer & Jorger, 2010). With a growing source of information publicly available, OSINT has taken on a greater urgency with the increases in nodes of information sources that can be unrestricted via the use of the surface and deep web (Glassman & Kang, 2012).

The introduction of OSINT to undergraduate and graduate students pursuing the information technology, cybersecurity, or criminal justice fields provides an excellent opportunity to engage with practical training. For those students pursuing law enforcement, the activity of OSINT can be a powerful approach to training future investigators (Larsen et al., 2023). OSINT techniques can include searching resources found in the surface web, deep web, social media, image and reverse-image, and mapping searches (Larsen et al., 2023).

The decision to not explore or search for relevant breach, attack, or hacking information on the Dark Web relevant to the NPO and NGO sectors was made purposely. The Dark Web may have ample amounts of relevant and unpublished information related to hacking that has transpired. However, the Dark Web also contains illicit information, knowledge, skills, and data related to hacking, including breaching accounts, such as social media and websites, access to malware, and steps to perform such attacks as Denial-of-service (Choi & Lee, 2022). This research activity includes academics, professionals, and students, and as such, by not entertaining the idea of scouring the Dark Web for open-source information on cyber-attacks, an ethical step is being demonstrated to students and users of this finalized dataset regarding using more formal published materials.

Alert Source	Purpose
Google Alert	"NGO" and "breach"; "NGO" and "hacking"; "non-profit" and "breach"; "non-profit" and "hacking"; "nonprofit" and "breach"; "nonprofit" and "hacking"; "relief agency" and "breach"; "humanitarian" and "breach; "humanitarian" and "hacking"; "non-governmental" and "breach"; "non-governmental" and "hacking"; "charity" and "hacking"; "charity" and cyber-attack"
INOREADER	"non-profit cyber-attack"; "non-profit cybercrime"; "non-profit breach"; "non-governmental organization cyber-attack"

Table 1: Automated Alert Terms Utilized

For this research activity in creating an available dataset, publicly available sources were utilized to search, discover, analyze, and determine if an entry was viable for inclusion in the database. The critical sources included Google Search, Google Scholar, INOREADER News Feed Creator, the digital library repositories of publications at the Kean University Digital Library, and the University of Cumberlands Digital Library. The use of the Google Alerts feature and function as a mechanism to be automatically notified of new publicly available information relevant to this

specific research effort was created to automate the process. The digital alerts were configured using key search terms outlined in Table 1. It is expected that as more sources are identified to contribute further to this research, the repositories will be added.

Initiation and Creation of an NPO and NGO Cyber Incident Reporting Dataset

The creation of the dataset was inspired by the lack of such a resource available in the public domain. Many sources of information related to cybersecurity and cybercrime incidents can be found via such resources as the FBI Internet Crime Complaint Center (IC3.GOV) web portal. Additionally, focused datasets related to specific types of cybersecurity incidents are available, as well as snapshots of activities in a variety of reports over the past many years. However, having a place for NPO and NGO organizations to reference historical records of attacks was found to be lacking. Hence, the vision of this instantiation of a data repository is to continue to grow and add value to these sectors. The expected importance of such data to quickly reference can be referred to by the NPO and NGO sector, as well as by those organizations that assess or audit this sector and by third-party partners that provide technology security services to protect them.

Dataset Collection Fields

The collection of historical data commenced in December 2023 and continues to the time of this writing. It is expected to continue going forward, with a different cohort of students trained and integrated each semester as new interns or academic assistants assigned to the Kean Center for Cybersecurity. As information was gained related to cybersecurity incidents that pertained to or affected non-profit and non-governmental organizations, the data was added to a secure web-based data portal. The initial set of fields utilized when recording the information found in the open source or publicly available avenues include the items found in Table 2. In addition to general demographics, fields related to the cyber incident were captured, and attempts to align with the 16 critical DHS sectors were made, as well as connections to TAG Infosphere's Cyber taxonomy (TAG Infosphere, 2024). The TAG Cyber taxonomy includes an organized list of significant categories aligned with cybersecurity approaches (TAG Infosphere, 2024). Additionally, we leverage and make a correlation between cyber-attacks and the Confidentiality-Integrity-Availability (CIA) triad. The CIA triad has helped define information system security in literature. It provides definitions of the three pillars that organizations can follow in the effort to safeguard their assets and technology infrastructure (Shiou et al., 2023). In relation to our categorizing which of the CIA triad elements relate to the NPO or NGO breach or cyber-attack, an assessment was made by the investigative team to make the category assignment.

Dataset Field	Purpose
Contributor First Name	Record contributor name.
Contributor Last Name	Record contributor name.
Contributor Email	Record contributor email.
Contributor Organization	Record contributor organization.
Incident Unique Identifier	We assigned a unique identifier.
Date of Incident	Date or approximate/estimated date of the incident.
Year	Year of incident – YYYY format.
Non-Profit/NGO Name	Name of NPO or NGO.
Non-Profit/NGO Country(s)	Country location(s) of NPO or NGO breached.
DHS CISA Critical Sector Targeted (if applicable)	Organization category alignment or included in one of the sixteen DHS CISA Critical Sectors.
Outside Sector (if applicable)	Organization category if outside of DHS CISA.
CVE Targeted (if available)	Targeted CVE (if applicable and available).
Attack Type	Type or genre of cyber-attack.
CIA Triad Element Effected	Recording of whether the Confidentiality, Integrity, or Availability (CIA) pillar was affected.
Location of OSINT Knowledge Source	Link or location of open-source intelligence article or information evident from the attack.

Dataset Field	Purpose
TAG Cyber Taxonomy	Record which category of the TAG Cyber reference taxonomy was affected or associated and included in the attack.
Upload of artifact about the incident	Additional artifact or evidence of attack.
Other Non-Profits/NGOs Targeted	Recording of other NPOs or NGOs affected by this attack.
Additional Information	Other miscellaneous information about the attack.

Table 2: NPCIR Dataset Fields (Codebook)

The process followed to discover and catalog the NPO or NGO cyber incident record included several steps. After first enabling and establishing automated alerts to when such information was newly available, the research team also did manual historical searches through the select information portals. Once discovered, a thorough read of the open source and publicly available articles or evidence was made, and it was determined whether the found information was relevant for inclusion in the dataset. Prior to adding the record to the dataset, members of the team manually considered each data element as outlined in Table 2 prior to addition to the repository. As part of the evaluation, considerations were made as to whether the attack was limited to the organization itself or other NPOs and NGOs.

Access to the resulting dataset is made available to individuals and companies after making a formal request via completing a web-based inquiry form. Upon receipt of the completed request form, members of the research and investigative team analyze the use case for utilizing the data repository. The repository is to be used for research defensive investigation, academic research, or potentially by the press if found useful given a specific applicable news story. The dataset is not permitted to be used to charge a fee or for any profit-making enterprise. Additionally, as the dataset continues to expand, it will be stamped with an increasing version label number and made available upon request and approval at least two to three times per year and provided in a PDF report.

5. RESULTS

In this first incarnation (version 1.0), the resulting data is presented after seven months of open-source intelligence gathering to determine the feasibility of the NPCIR data repository. It is anticipated that after each instantiation of the data repository, the dataset will grow, and it is expected that at least two versions with the most updated results included will be generated annually and provided for open access. A total of *N* = 168 cybersecurity incidents have been discovered thus far focused on the NPO and NGO organizations. The recorded year with the most documented and discovered attacks was 2023, and the earliest documented was 2011. The most attacked NPO and NGO country was the United States, with an abundant number of countries being recorded. The CIA pillars most affected in the recorded attacks, which could include multiple pillars, included (1) Confidentiality at 81%, (2) Integrity at 49%, and (3) Availability at 41%. The most targeted or DHS CISA-aligned sector affected by cyber-attacks included those from the Healthcare and Public Health sectors, reporting 45.5% of all incidents discovered. The resulting summarized data can be found in the following Figures: 1, 2, 3, 4, and 5 with additional descriptive statistics.

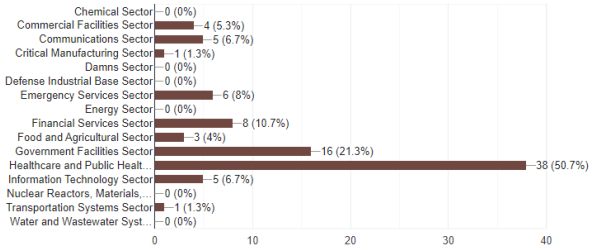

Figure 1 DHS CISA Targeted Sectors

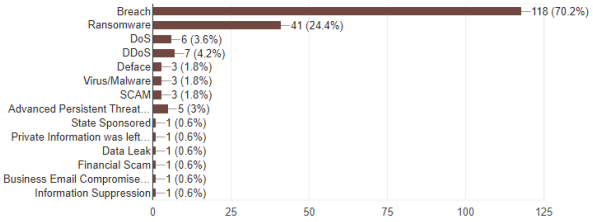

Figure 2 Attack Type

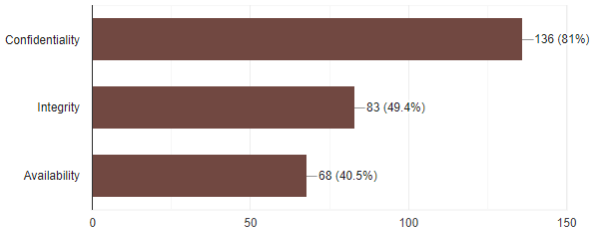

Figure 3 CIA Affected

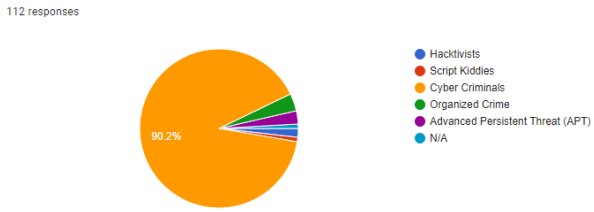

Figure 4 Threat Actor Type

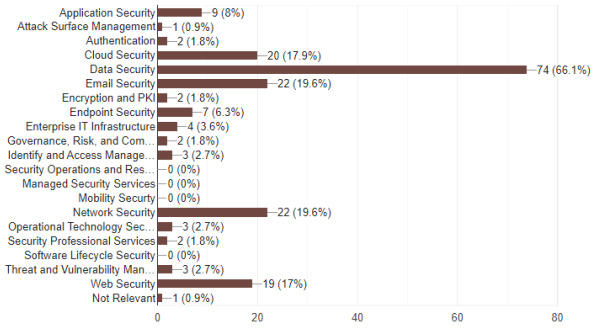

Figure 5 TAG Cyber Reference Taxonomy

One of the descriptive findings was that the information collected and discovered regarding non-profits that have been hacked was more likely to be categorized as "breached" as a hacking approach in the attack, resulting in over 70% of the discovered attacks. This finding supports the previous finding of a quantitative study that resulted in a significantly higher number of breaches due to unauthorized access to non-profits via breaches, and for-profits experienced breaches in higher volume due to theft (Ignatovski, 2023). The next most common attack type was found to be "ransomware" at 24% (Ignatovski, 2023).

6. DISCUSSION AND IMPLICATIONS

In relation to operating an organization, NPOs and NGOs are no different than most for-profit businesses. Organizations with an NPO or business mission will aim toward being efficient, innovative, and effective by considering the use of information technology solutions in their operations. Just the same as larger corporations, the NPO and NGO environment will be involved in generating technology solutions and using modern cloud-based solutions, such as Microsoft Azure (Souidi et al., 2015). Additionally, as part of the data collection research efforts in NPOs and NGOs, innovative self-report survey systems or other novel, groundbreaking solutions may be offered (Falb et al., 2016; Mierzwa et al., 2016; Savel et al., 2014). In essence, every time a new information technology or web-based or Internet-connected product is provisioned, there will be the potential for cybersecurity attacks.

Several essential learning items emerged as a result of this exercise. In one case, many NPOs and NGOs may not necessarily align with the CISA's sixteen critical infrastructure areas, and as a result, a field to categorize areas outside the sectors was added. As this activity and research continue, these critical areas outside the CISA sector may grow. At this time, the additional NPO- or NGO-focused categories include Humanitarian Aid, Education, Food Security, Support Democracy, Political Organizations, Scientific Services, Technical Services, and Arts/Entertainment Services. For students who may be unsure of the relevance of cybersecurity to varied sectors of industry and focus, this activity provided excitement for them in understanding the practicality of this approachable activity. It is envisioned that a new set of interns will be assigned each semester to carry this effort through a sustained model. Without providing routine attention to this OSINT activity, there is the potential to no longer be viable.

7. CONCLUSION

It can be overwhelming for a cybersecurity student, researcher, incident responder, cyber risk manager, or defensive technical cyber expert to zero in on relevant information affected in the specific sector one operates. With cybersecurity and cybercrime being very fast-moving targets, having valuable resources that are more attuned to one's industry or sector can be an appreciated asset in information security and cybersecurity awareness. The NPO and NGO environment has often relied on general-purpose cybersecurity repositories to help them contend with the aftermath of attacks and defend against upcoming potential attacks. Cybersecurity analysts and researchers will rely on mixed or more than one dataset when aiming to protect their organizations from attacks, and this activity helps to draw attention to those in the NPO and NGO communities.

This first version and initial student-focused activity and research were started to help students involved in a cybersecurity internship. The students were from a variety of disciplines, including information technology, computer science, and criminal justice. This practical investigation activity has helped the students to grasp better and understand the landscape of research for the purpose of preventing cybersecurity and cybercrime attacks. The knowledge, skills, and abilities provided to the students included understanding the DHS CISA sector categories, introduction to OSINT, tracking and tracing threat intelligence, practical assessment of the CIA triad, concepts of security ethics, and using nontechnical skills of collaboratively working on a tangible project. This effort was found to be feasible and will continue to be pursued with future students.

8. LIMITATIONS

The discovered and added cybersecurity incidents in the NPO and NGO sectors or communities were, for the most part, done manually by humans, with the exception of automated alerts. This is a limitation and demonstrates that the process may be inefficient given the steps necessary. This human-level interaction creates a limitation, and perhaps future evolutions to the product could be completed with artificial intelligence bots or automated scripts. Additionally, there is the potential that previous evidence of cyber-attacks against the NPO or NGO communities was removed from the public domain or surface web and not able to be cataloged, which would not appear in this repository dataset.

9. FUNDING

The author (s) received no financial support during the course and activity of this research and publication.

10. ACKNOWLEDGEMENTS

Part of the inspiration for pursuing this activity was the interest of students who were assigned to the Kean Center for Cybersecurity as part of an internship research project. Hearty thanks to students Heni Patel, Gurdeep Singh and Caitlin Chiodo, for their involvement in the practical cybersecurity exercise and research. This outreach activity is in favor and support of the National Security Agency Center of Academic Excellence Cybersecurity Defense (NSA CAE-CD) outreach action. Such outreach and student-faculty involvement activities are advocated and expected in yearly efforts. The authors are genuinely grateful to the Kean University Office of Career Services for their excellent outreach to partner students with faculty at the university that align with student interests.

11. REFERENCES

Choi, M., & Glassman, M. (2017). What it means to be a citizen in the internet age: Development of a reliable and valid digital citizenship scale. *Computers & Education, 107*, 100-112. https://doi.org/10.1016/j.compedu.2017.01.002

Choi, K. S., & Lee, C. S. (2022). In the Name of Dark Web Justice: A Crime Script Analysis of Hacking Services and the Underground Justice System. *Journal of Contemporary Criminal Justice, 39*(2), 201–221. https://doi.org/10.1177/10439862231157520

CISA.GOV. (2022a). CISA Central Reporting Operations Guide. As retrieved on December 26, 2022, from: https://www.cisa.gov/sites/default/files/publications/CISA_Central_Operations_Branch_Slick%20Sheet_508c.pdf

CISA.GOV. (2022b). Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) Fact Sheet. As retrieved on December 23, 2022, from: https://www.cisa.gov/sites/default/files/publications/CIRCIA_07.21.2022_Factsheet_FINAL_508%20c.pdf

CommunityIT Innovators. (2023). *2023 Nonprofit cybersecurity incident report.* https://communityit.com/2023-nonprofit-cybersecurity-incident-report/

Cyber Peace Institute. (2021). *Playing with lives: Cyberattacks on healthcare are attacks on people.* https://cyberpeaceinstitute.org/report/2021-03-CyberPeaceInstitute-SAR001-Healthcare.pdf

Ermicioi, N., & Liu, M. X. (2022). Cybersecurity in nonprofits: Factors affecting security readiness during Covid-19. *SAIS 2022 Proceedings, 18*. https://aisel.aisnet.org/sais2022/18

Falb, K., Tanner, S., Asghar, K., Souidi, S., Mierzwa, S., Assazenew, A., & Stark, L. (2016). Implementation of Audio-Computer Assisted Self-Interview (ACASI) among adolescent girls in humanitarian settings:

feasibility, acceptability, and lessons learned. *Conflict and Health*, *10*(1), 1-8.

Friedman, S., & Mitchell, C. (2022). Former Federal CISO calls for early CISA workshop as industry leaders seek a place in shaping incident reporting rules. Inside Cybersecurity. Arlington.

Glassman, M. (2013). Open source theory. 01. *Theory & Psychology*, *23*(5), 675-692. https://doi.org/10.1177/0959354313495471

Glassman, M., & Kang, M. J. (2012). Intelligence in the internet age: The emergence and evolution of Open Source Intelligence (OSINT). *Computers in Human Behavior, 28*(2), 673-682. https://doi.org/10.1016/j.chb.2011.11.014

Harry, C., & Gallagher, N. (2018). Classifying cyber events. *Journal of Information Warfare*, 17(3), 17-31.

Ignatovski M. (2023). For-profit versus non-profit cybersecurity posture: breach types and locations in healthcare organizations. Health Information Management Journal, 0(0), 1-8. doi:10.1177/18333583231158886

Internet Crime Complaint Center. (2022). *Federal Bureau of Investigation Internet Crime Report 2021*.

Kim, Y., Glassman, M., & Williams, M. S. (2015). Connecting agents: Engagement and motivation in online collaboration. Computers in Human Behavior, 49, 333-342. https://doi.org/10.1016/j.chb2015.03.015

Kouper, I., & Stone, S. (2024). Data sharing and use in cybersecurity research. *Data Science Journal, 23*(3). 1-19. https://doi.org/10.534/dsj-2024-003

Kuznetcova, I., & Glassman, M. (2018). Rethinking the use of multi-user virtual environments in education. Technology, Pedagogy and Education, 29(4), 389-405. https://doi.org/10.1080/1475939x.2020.1768141

Lambert, J. (2021). Microsoft Digital Defense Report. Retrieved on March 6, 2024 from: https://www.microsoft.com/en-us/security/blog/2021/10/25/microsoft-digital-defense-report-shares-new-insights-on-nation-state-attacks/

Larsen, O. H., Ngo, H. Q., & Le-Khac, N. A. (2023). A quantitative study of the law enforcement in using open source intelligence techniques through undergraduate practical training. *Forensic Science International: Digital Investigation, 47*, 1-11. httpsS://doi.org/10.1016/j.fsidi.2023.301622

Mierzwa, S. J., & Klepacka, A. (2023). Practical Approaches and Guidance to Small Business Organization Cyber Risk and Threat Assessments. *Journal of Strategic Innovation and Sustainability*, *18*(2). https://doi.org/10.33423/jsis.v18i2.6255

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 & Cybercrime, 3*(2), 48-61. https://www.doi.org/10.52306/03020420BABW2272

Mierzwa, S., Souidi, S., & Savel, C. (2016). On selecting an appropriate customizable electronic self-report research technology. *Procedia Engineering, 159*, 66-71. https://doi.org/10.1016/j.proeng.2016.08.065

Morris, S. (2000). Defining the nonprofit sector: Some lessons from history. International Journal of Voluntary and Nonprofit Organizations, 11(1), 25-43.

Neprash, H., McGlave, C. C., Cross, D. A., Vimig, B. A., Puskarich, M. A., Huling, J. D., Rozenshtein, A. Z., & Nikpay, S. S. (2022). Trends in Ransomware Attacks on US Hospitals, Clinics, and Other Health Care Delivery Organizations, 2016-2021. *JAMA Health Forum. 3(*12). doi: 10.1001/jamahealthforum.2022.4873.

Neprash, H., & Rozenshtein A. Z., (2023). New Data Quantifies Ransomware Attack on Healthcare Providers. *Lawfare. Institute in Cooperation with Brookings*. As retrieved on January 10, 2023, from: https://www.lawfareblog.com/new-data-quantifies-ransomware-attacks-healthcare-providers

Rege, A. (2023). "Critical Infrastructure Ransomware Attacks (CIRA) Dataset". Version 12.9. Temple University. Online at https://sites.temple.edu/care/cira/. ORCID: 0000-0002-6396-1066.

Salamon, L. M., & Anheier, H. K. (1992). In search of the non-profit sector: The question of definitions. Voluntas, 3, 125-151.

Savel, C., Mierzwa, S., Gorbach, P., Lally, M., Zimet, G., Meyer, K., Souidi, S., & Adolescent

Trials Network for HIV, & Interventions, A. (2014). Web-based, mobile-device friendly, self-report survey system incorporating avatars and gaming console techniques. *Online journal of public health informatics*, *6*(2), e191. https://doi.org/10.5210/ojphi.v6i2.5347

Shiou, W. L., Wang, X., & Zheng, F. (2023). What are the trends and core knowledge of information security? A citation and co-citation analysis. *Information & Management, 60*(3), 1-21. https://doi.org/10.1016/j.im.2023.103774

Sobers, R. (2024). 161 Cybersecurity statistics and trends [updated 2023]. Varonis. Retrieved on March 6, 2023, from: https://www.varonis.com/blog/cybersecurity-statistics

Souidi, S., Boccio, D., Mierzwa, S., & Aguilar, J. (2015). The feasibility of using Microsoft Azure infrastructure for a monitoring and evaluation system solution in Sub-Saharan Africa. IEEE Global Humanitarian Technology Conference. IEEE, 226-232.

TAG Infosphere. (2024). TAG Cyber Taxonomy. As retrieved on February 28, 2024, from: https://tag-infosphere.com/service/cybersecurity/taxonomy

Verizon. (2022). Verizon Data Breach Investigations Report 2008-2022. A retrieved on December 6, 2022, from: https://www.verizon.com/business/resources/T34a/reports/dbir/2022-data-breach-investigations-report-dbir.pdf

Walton, J. (2017). The role of non-governmental organizations in vaccine development and delivery. International Journal of Health Governance, 22(3), 152-160. https://10.1108/IJHG-02-2017-0006

Willetts, P. (2002). What is a non-governmental organization? *Conventions, treaties and other responses to global issues*, *2*(11), 229-248