Reaching an Underserved Population in Communities: Project Xander – Cybersecurity for NonProfits

Gregory White, Ph.D.
Professor of Computer Science, UTSA
Greg.white@utsa.edu

Abstract

Cyber criminals continue to look for new targets which they can exploit. A recent addition to their list of targets are nonprofit and faith-based organizations within communities. These organization generally do not have the budget to hire a cybersecurity professional or pay for cybersecurity services. A program to reach this sector to assist them with their cybersecurity posture was launched called Project Xander. This program is designed to utilize students from area colleges and universities to provide assessment and consulting services for organizations within the sector. The pilot program was run in the 2021-2022 academic year and was successful and is now being expanded to include other communities and academic institutions. It addresses a need in communities in a sector that has been underserved and that has historically not had the resources to implement robust cybersecurity programs.

Keywords: Cybersecurity, education, nonprofit organization, assessments

1. Introduction

Cybercrime has been increasing steadily over the last decade and reached $6 trillion in damages worldwide in 2021. [Vojinovic, 2022]. Cyber criminals, interested in maximizing their profit, look for easy targets to exploit. As cybersecurity postures have improved in government, the critical infrastructures, and industry, some criminals have switched their target focus to sectors with targets that are easier to exploit.

> *For any cybercriminal, the ideal victim is not an organization with vast resources but one that is easy to hack and has a lot to lose when its network is breached. Unfortunately, most NGOs and nonprofits more than fit this bill.* [Shavell 2021]

With the possible exception of very small rural communities, all communities will have a variety of nonprofit and faith-based organizations that citizens may donate money to. Financial information on the organizational computer systems may very well be stored on these systems. These organizations have very limited budgets and have not historically spent much on cybersecurity.

> *According to a survey by CohnReznick, more than two-thirds of nonprofits failed to assess their levels of cybersecurity risk. And a 2018 study by NTEN found that eight in ten nonprofits didn't have a cybersecurity policy in place.* [Shavell, 2021]

While it may seem at first that these organizations may not be likely to experience a cyberattack, this is not the case. In the U.S. these organizations have indeed been targeted by cyber criminals who know that they are likely not to have adequate cybersecurity controls in place. A number of attacks on nonprofits have occurred in the past:

> *For some recent examples of such attacks, reference the Utah Food Bank incident (wherein more than 10,000 individuals' personal information submitted via the donation website was exposed by a hacker), the attack affecting the International Committee of the Red Cross (a targeted attack on the ICRC servers that compromised more than 500,000 highly vulnerable individuals' personal data and confidential information), the YMCA of Greater Charlotte incident (a ransomware attack on their servers that affected an unknown number of users), the ShopGoodwill platform incident (a website vulnerability that led to a data breach that affected the accounts of customers using its e-commerce auction platform), or the breach that affected the Partnership HealthPlan of California, a nonprofit organization that manages health care for counties in California (a ransomware attack that led to the ransomware group stealing private data for roughly 850,000 members, including social security numbers).*[Maimone-Medwick, 2022]

URI: https://hdl.handle.net/10125/102841
978-0-9981331-6-4

While it is not the responsibility of a community to secure all nonprofit and faith-based organizations, it does behoove the community as a whole to see that these entities are secure. Since many citizens may have donated money to nonprofit or faith-based organizations which in turn may have stored personal financial information such as credit card numbers on donors, it would be in the interest of the community to ensure that the information is stored in a secure manner. These organizations, however, are generally on a limited budget and do not have the money to spend on cybersecurity professionals and in fact may not even have full-time IT employees. Communities may have an entity that can help nonprofit and faith-based organizations and that would in fact benefit the entity as well. This entity would be a college or university that teaches cybersecurity courses.

2. Providing Hands-on Experiences

Two decades ago, the idea of teaching college students skills that would enable them to conduct penetration tests and security assessments was often viewed with much apprehension. The fear expressed by many administrators was the classes would be training the “next generation of hackers”. Over the last few decades, this fear has largely subsided and providing students with labs and tools to become familiar conducting penetration testing and assessments is generally accepted as a reasonable academic endeavor – provided sufficient time is spent on ethics to emphasize when it is appropriate to use the skills. This is evidenced by the posting of tools and information by the Department of Homeland Security to encourage academia “to increase cybersecurity awareness, incentivize cybersecurity, encourage the adoption of best practices, and implement a shared sense of responsibility for cybersecurity at universities and colleges.” [DHS/CISA, 2022]

Providing students assignments addressing security assessments and a lab environment in which to gain experience with vulnerability scanning and exploiting tools is a good experience for students in classes. This experience is not just for 2-year programs which are often focused more on training skills as opposed to education. These tools also provide insight into system and network aspects that are discussed in classes. They consequently make sense to include in labs at the 4-year level to illustrate points described during lectures.

Having a class provide assessment and penetration testing services for a real-world organization provides more than just an understanding of specific tools, policies, procedures, and processes. It valuable for students to experience what organizations actually face. It is easy for students to discount stories about “little yellow stickies” with userids/passwords written on them until the first time they actually see an example of this poor security practice. Also, students in class live in a world where things may seem to be very clear. If there is a security vulnerability in an application for which a patch exists, most students will see this as a simple issue – patch the system. In the real-world, however, things are not as simple. A patch may result in another piece of software critical to the organization failing in some way. [NCSC, 2022] Thus, another way to mitigate the vulnerability will need to be implemented. For students in a security class, the level of importance of cybersecurity is another issue that may often seem clear to them – cybersecurity is so important that it should always receive a significant amount of time and resources. For real-world organizations, however, cybersecurity may not be the priority that students feel it should be. Organizations have to make basic decisions on budgets and personnel and how much to spend on cybersecurity. For all of these reasons, working with real organizations outside of a lab environment provides valuable experience.

A final advantage of a real-world experience occurs as students gain insight into issues facing organizations which can lead to ideas that translate to research projects at both the undergraduate and graduate levels.

The challenge of teaching cybersecurity sills to students was discussed by Seda et. al., in their paper on adaptive learning. [Seda, 2022] They point out the challenge of conducting hands-on cybersecurity training that would meet the needs of all students. They went on to point out instructors can help students interactively, but it is only feasible in relatively small classes. [Seda, 2022] They suggest improving student skills can be accomplished using intelligent tutoring systems and an adaptive learning environment. While this is true, a different approach, the incorporation of multiple team mentors, was utilized to provide the individualized training needed by students in Project Xander.

(It should be noted that throughout this paper the term “assessment” is used to refer to the activities conducted by the students. In the cybersecurity field terms such as assessment, audit, and test have very specific meanings. This is fully acknowledged by the author though the term “assessment” is used sometimes interchangeably with these other terms in this paper. The assessment conducted on the various organizations consisted of a variety of activities that would fall into one or more of these areas and depended on the desires of the organization and the maturity of their cybersecurity program. What was accomplished was based on the needs of the individual organizations.)

3. Project Xander

Addressing both the academic learning experience for students and nonprofit cybersecurity needs is the goal of **Project Xander**. Xander is a shortened version of the name Alexander. Alexander in turn means "defender of men" or "one who assists men". The goal of the project is to help nonprofit and faith-based organizations defend their cyber assets from cyberattacks. In doing so, it also aimed at assisting these organizations in improving their cybersecurity posture and implementing improved cybersecurity programs. On the academic side, the goal was to expose students to a learning experience that would provide them more insight into the real-world cybersecurity experience of organizations, especially those that most likely had little to no cybersecurity implemented.

The concept proposed for the project was to link student teams with nonprofit and faith-based organizations within the community. One early concern was the project should not be in competition with cybersecurity vendors. The project did not want to be taking revenue away from vendors. This was another reason that nonprofit and faith-based organizations were targeted instead of working with local government or industry though in some communities both of these entities might suffer from the same budgetary issues experienced by the nonprofit and faith-based communities and could be included in the project.

As the planning progressed, the thought was to have the class conducting the assessment be a capstone course in cybersecurity or a course focused on cybersecurity assessments. As planning progressed, the project recognized the need by the organizations to also receive assistance in implementing recommendations that might result from the assessment. The assessment portion also was divided into two different major projects. The first evolved into a "paper assessment" or security audit and related activities, the second would be a more technical assessment such as a penetration test, scanning for wireless access points, or cracking of wireless encryption.

Timing was an issue that had to be considered from the beginning of the planning process. A penetration test or an audit/assessment conducted by a cybersecurity vendor could be accomplished in just a few weeks from in-brief to out-brief. With students accomplishing the tasks the organizations needed to understand the time to complete the work would take longer because of competing projects from other classes the students would be enrolled in. Not only did this need to be stressed with the organizations but also the amount of time that the organization needed to be able to devote to the students in order for them to accomplish what they needed to do had to also be conveyed to the organizations. In fact, the students might very well need additional time with individuals from the organization since they did not have experience in conducting tests and assessments. It was considered a fair tradeoff for the organization, however, since they would be obtaining the services for free.

To prepare the students, the instructor of the course(s) would need to make sure they knew what was involved in an assessment and what tools might be used in a more technical assessment such as a penetration test. In terms of the penetration test, some preliminary labs would probably be needed to provide the students an opportunity to use the tools they would be using for the test. It was envisioned that all tools and materials used in both the assessment and testing portions should be publicly available such as Metasploit for the technical tool as it includes a number of other tools useful for a penetration test and includes exploits for items that are discovered.

For the audit/assessment, there are a number of documents that can be found on the Internet that provide suggestions as to what an assessment might include. Some additional guidance was supplied by the instructor to focus the student efforts but there is a lot of information on the Internet that can aid security professionals and the instructor wanted the student to recognize and experience this. The goal of the assessment would be to determine what the current security posture was for the organization and to make recommendations on how to improve it. The guidance that can be found on the Internet can be quite extensive and is often intended for large organizations. The target organizations in this case needed to be kept in mind. The nonprofit and faith-based organizations would be local entities and not the headquarters for a nonprofit organization such as the American Red Cross or American Cancer Society. The organizations would be small and would likely not have anybody well-versed in cybersecurity. Thus, the materials used should be targeted for smaller organizations and should not require an extensive background in cybersecurity. The recommendations that resulted from the data gathered during the assessment through interviews and a checklist audit would need to be tailored to be applicable to the target organization, their environment, and their level of understanding of cybersecurity. This most likely would mean that recommendations should be as easy to implement as possible and should be no- or low-cost items. Since the organizations could be quite varied, guidance the students should be familiar with could start with items such as the following:

- CIS Critical Security Controls
- CIS Guide for SMEs
- CIS Risk Assessment Method (RAM)
- NIST Cybersecurity Framework

- NIST IR 7621r1 (The Fundamentals)
- NIST SP 800-171r2 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
- NIST SP 800-53r5 Security and Privacy Controls for Information Systems and Organizations
- NIST SP 800-60 vol 1 guide for Mapping Types of Information and Information Systems to Security Categories
- NIST SP 800-60 vol 2Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories
- FIPS 199 Standards for Security Categorization of Federal Information and Information Systems
- FIPS 200 Minimum Security Requirements for Federal Information and Information Systems

This list is just a sample of what students could be made familiar and additional guidance could be provided for which were most applicable for them in their situation could be provided by both the mentor and the instructor. A number of the documents are guidance provided to U.S. federal agencies which the nonprofit and faith-based organization will not be part of. The information contained in these publicly available documents, however, provide a good foundation for what might be part of an organization’s cybersecurity program no matter the sector of nation within which the organization resides. The documents cover several types of information. There are a number of documents that will provide some background on various security requirements that an organization should have in place. These do NOT need to be implemented in their entirety as the needs of the organization and their current security posture will dictate the recommendations that will be made. A good example of this is the NIST Cybersecurity Framework (CSF) which includes a large amount of information and a tremendous list of possible resources from which to obtain additional information. This is a very large document, however, and to try and have a small organization incorporate all categories and subcategories outlined in the CSF would be too overwhelming. Instead, an understanding of the five core functions (Identify, Protect, Detect, Respond, and Recover) could be discussed and recommendations and findings grouped to cover these functions at the appropriate level.

The Center for Internet Security (CIS) documents in particular will be very useful in helping the students determine what sort of items to include in the checklist they will use.

To be of the most benefit for both the student teams and the organizations involved, a well-defined set of deliverables should be agreed upon. The list of deliverables will ultimately vary depending on the needs of the organization, but the following should be included by every team:

- A non-disclosure agreement signed by each student team and the organization. The purpose of this is to stress to the students that anything they learned about the organization may not be disclosed to anybody other than the instructor and the organization itself. It also provides a level of assurance for the organization that their information will remain confidential.
- An In-briefing for the organization that includes a discussion of the types of things that could be included in the assessment, the approximate timeline, a list of information the organization will need to supply, and an approximation for the amount of time that the students would need with a member of the organization to conduct the identified tasks. Points of Contact for both the team and the organization as well as contact information for the instructor should also be supplied.
- The audit checklist the students would use. This could be one downloaded from the Internet and modified and should include the appropriate citations. It might also consist of a checklist developed by the students from information they gleaned from other sources and combined to fit the needs of their organization.
- A final report with findings and recommendations for the organization. The report should include items such as:
  - Results (analysis) of the completed checklist
  - Evaluation of all security-relevant policies the organization has (or should have) implemented
  - Evaluation of the organization’s cybersecurity training and awareness program.
  - Evaluation of backup, contingency, disaster, continuity of operations or similar plans as appropriate.
  - Copies of all “raw data” used in the evaluation to produce the recommendations. These can be included as appendices.
- An out-brief that would provide a synopsis of what occurred, findings (both good and bad), and recommendations.

The reason for these deliverables is that ultimately it is how well the students have interacted with their organization and the value of the findings and recommendations that will determine the success of their efforts. Since some materials provided by the organization could be considered of a sensitive nature as well as the report on findings and recommendations, a secure mechanism for transmission and storage of documents should be provided. The students should also be prohibited from retaining a copy of any document that had identifying elements in it. Students should be allowed to generate a sanitized version of the report with all identifying elements removed that they could keep for their own records.

4. Implementation in 2021-2022 Courses

A smaller implementation of a similar program had been included in an earlier course at the university but for the 2021-2022 academic year the assessment assignment was to be inserted into a two-course sequence with the audit and evaluation of policies and training to be conducted in the Fall and the penetration and other technical evaluations to be conducted in the Spring. With the Covid-19 pandemic causing courses to be taught virtually, this also meant that the assessments and testing would be conducted virtually.

4.1. Courses

The two courses in which the project was to be conducted were the Computer Science 3433 Principles of Cybersecurity in the Fall and the Computer Science 4673 Cyber Operations course in the Spring. Both courses are required courses in the Cyber Operations track and as a result were mapped to specific requirements for the NSA Center of Excellence in Cyber Operations designation. While the project fit nicely into the lab portion of both classes, it did mean that neither course could focus entirely on conducting an assessment, audit, or penetration test. In other words, the courses could not simply be switched to become a course on risk assessments, risk management, or “ethical hacking”.

The Cyber Operations track is popular, and the online Principles of Cybersecurity course started with 80 students but a wait list with several dozen students quickly occurred. The course was opened to allow additional students and ultimately the course ended up with 122 students. This was going to be a problem because in the previous course where an assessment was conducted on a small business, a government organization, and a nonprofit organization the class size was small enough to allow the instructor to oversee and advise each of the teams conducting the assessments. With 122 students this was not going to be possible. Either the team sizes would have to average 20 students each or additional assistance for the students would need to be obtained. A team size of 20 students would not work as trying to organize meetings that both the organization being assessed and the team members would be able to attend would almost certainly mean some of the students would not be able to attend. Additionally, a team with 20 members would almost certainly result in team members not participating fully and none of the students would be able to experience all parts of the assessment. The decision was therefor made to reach out to cybersecurity professionals in the community and ask for assistance. The idea was to recruit enough professionals so that a “mentor” could be assigned to each of the teams. With this in mind, the maximum number of teams could be increased and would become a function of the number of professionals that could be recruited and the number of organizations that desired to have an assessment conducted.

4.2. Mentors

The mentors were an absolutely essential element of Project Xander. Without them the number of organizations that could be covered in a semester would have been greatly reduced. In the initial implementation of the project, we were very fortunate to have the MITRE Corporation step up and volunteer to provide mentors. They supplied half of the mentors that were involved in the project. The other half consisted of cybersecurity professionals from a variety of organizations within the community. Some were from cybersecurity vendors, others were from non-cybersecurity organizations but who employed cybersecurity personnel. A big part of the success of the project was due to the willingness of both the mentors, who devoted time to the student teams, and the organizations they were from and who allowed their employees to devote time to the project. The mentors supplied the experienced leadership that was incredibly valuable for the teams.

Each team was assigned a mentor who was very involved in advising the team. A critical rule for the mentors was they were an advisor for the students, they were not directly involved in conducting any part of the assessment itself. They were there to answer questions the students had about the assessment and to provide suggestions based on their own experience as cybersecurity professionals.

The mentors were provided with some initial guidance to help them plan for how best to work with the teams. The mentors were provided with a description of the objective for the project in a bit more detail than was provided to the students – for example what did the instructor hope that the students would experience as a result of the project. The mentors were also provided with some pointers to provide the students should they become stuck on some aspect of the project. The pointers were to be provided after the students attempted to solve whatever the issue was on their own. It was important that the mentors didn't immediately jump in with answers to any question but rather let the students attempt to find the answers on their own first. At the same time, it was important that the teams weren't left hanging for an extended period of time because we didn't want them to become discouraged.

In addition to being accessible for questions the students might have, the mentors were asked to provide some specific assistance which included:

- Initial contact with the organization: Before the student team contacted their organization the mentors were asked to first speak with the organization to ensure that the organization was aware of the commitment required of them for the assessment to occur and to answer any questions on what might occur during the assessment. The mentor, as a cybersecurity professional, would be much better situated to allay any fears the organization might initially have.
- A relatively simple, but very important task, was for the mentors to collect the signed Non-Disclosure Agreements (NDA) from the students. The mentors were asked to collect these so they knew when the team was prepared to communicate with the organization.
- Schedule and conduct an initial team meeting with the students to learn their backgrounds and to discuss the assessment process. Each team was required to select a team captain and an individual who would brief the organization. This could be the team captain, or it could be another individual with good oral communication skills. The team could also decide to split the briefing up between different members, but this was not required as part of the project and could, in fact, be distracting for the organization by breaking up the initial briefing and disrupting the flow.
- The team was responsible for developing an initial in-briefing to present to explain the steps of the assessment and what would be required. The mentor was asked to assist the individual(s) making the presentation to ensure they were ready
- The organizations were presented with a variety of items that could be part of the assessment and were asked to select those that were most applicable and that they desired. The mentors were asked to be ready to assist the teams with guidance on how to conduct the different parts and to provide pointers as to where they could find more information.
- A final report with recommendations was part of the deliverables for the organization. The mentor was not supposed to write any part of the report, but were asked to review the report and make recommendations on ways that it could be improved and could be made as useful as possible for the organization.
- Just as there was an initial in-briefing provided to the organization, there was a final out-briefing as well. Again, the mentor was not supposed to create the briefing nor to conduct any part of it but were asked to review what the team prepared and make recommendations on ways to improve it.
- Part of the original plan for the project was after the assessment was conducted and the report was delivered, the students were to help the organization actually implement the recommendations where possible. The mentor was again not responsible for taking part in any of the improvements but was asked to be available to provide guidance on what might be needed and where the students could find more information.
- At the conclusion of the project for the semester, mentors were asked to provide feedback to the course instructor on any recommendations they might have to improve the program and the experience for the students and the organization assessed. While the mentors were not responsible for grading the students, feedback was also asked to provide insight into the team and its members for the instructor.

From the list of tasks the mentors were asked to accomplish, it should be easy to see they were primarily there to ensure the students had somebody to go to for guidance and that there was somebody who could oversee the efforts of the various teams to ensure that the organizations received a valuable assessment. The mentors were not responsible for resolving any conflicts or issues that arose but were asked to inform the instructor should a problem occur with either the student team or the organization itself.

4.3. Organizations

A major aspect of the project was to work with the community to identify organizations that could benefit from a cybersecurity assessment of some sort and who didn't have the personnel or budget to be able to have an assessment conducted. Nonprofit and faith-based organizations fit this description and are found in all but the smallest of communities.

Working with the city, we came up with a list of over 230 nonprofit organizations plus some additional faith-based organizations within the community as well. This was obviously more than could be handled by the students in the course. The city asked the list of organizations who whether they would be interested in having a cybersecurity assessment be conducted on their network/systems. A brief explanation was included as to what this meant so the organizations could decide whether they were interested or not. A large number expressed an interest and additional information was provided to them so they had an idea about the timeframe for the assessments and the amount of time it would take. Ultimately 21 faith based organizations and charities became part of the project.

One of the items that was immediately developed for use in the project was a Non-Disclosure Agreement (NDA) for the students to sign. This is a common part of a commercial assessment where a vendor obtains sensitive security-related information about an organization, and this was explained to the students. It was also important to stress to the students what they were engaged in went beyond a classroom project but was an actual security-sensitive project that could impact an organization negatively if certain information were to be exposed to potential criminal elements.

An alternative assignment was provided for those students who did not wish to participate because they were not willing to sign the NDA or who could not participate in a group project as a result of other commitments. Less than 10 out of the class of 122 students elected to not participate.

Students were provided a list of the organizations for which assessments were going to be conducted and they had the option to state a preference for working with a specific organization or if there was a specific organization they did not want to work with. The instructor asked for a reason for either preference so a decision could be made whether to honor the request. The instructor wanted to avoid a situation where some organizations had a large number of students who wanted to work with them or conversely an organization who nobody wanted to work with. At the same time, if, for example, an individual was a member of the congregation for a church that was to be part of the assessment, to help facilitate communication between the team and the organization it was felt to be desirable to assign the student to the team. It was also deemed equally as important to not assign a student to an organization that they had specific objections to or that was not aligned with any strong personal beliefs they might have. A student, for example, who was a member of one political party and who didn't want to be assigned to a team conducting an assessment on an organization that had conflicting viewpoints had their request honored. It was fully realized that in a real-world situation this sort of thing might come up and the security professional would be asked to participate in an assessment anyway. Since this was a student project, however, it was decided to avoid any potential issues and simply honor such requests.

Ultimately, the list of organizations that started with the project included local entities affiliated with national organizations (such as Goodwill), groups dedicated to medical research and support for individuals suffering from specific medical issues (such as cancer), groups supporting youth activities, support groups for women, support groups for children, and religious congregations.

4.4. Included in the Assessments

As was previously mentioned, the specific details on what was accomplished for each individual organization depended on the desires and current security posture of the organization.

Having said that, most of the organizations had little to no cybersecurity policies, processes, procedures or technology. This allowed the instructor to focus on some common elements all of the teams could include in their offerings to organizations. This included:

- An audit. Audits are based on an evaluation against a specific set of standards. Specific sectors have regulatory requirements that cause audits for them to address these requirements. In the case of the organizations assessed by the student teams, however, basic security checklists were developed and used. Part of the student assignment was to evaluate checklists they found on the Internet and to either use one they felt was appropriate or to develop one that would include the elements that would be important for their organization. The thoroughness and appropriateness of the checklist proposed was graded BEFORE it was used in the assessment of the organization so students could receive feedback before they started their assessment.
- Evaluation of the cybersecurity training and awareness program. Most of the organizations did not have any real training or awareness

program so this provided the students with a very tangible deliverable they could provide. Similar to the checklists, there are a number of security training resources available on the Internet which the students could recommend or utilize to develop their own version applicable to their organization.

- Security-related policies. Few organizations had any written policies though some had verbal or "well understood" policies for various computer and network aspects. Here again was an opportunity for students to provide materials to help their organizations develop their own written policies regarding items such as password creation/management, acceptable use of resources, protection of personal and sensitive information, data backup and retention, use of personal systems for business purposes, and remote access. There are plenty of examples of policies on the Internet that the students could provide as examples organizations could then implement.
- Incident response and continuity of operations plans. None of the organizations had any established, well-documented policies on what to do in the event of a cybersecurity incident. None had any established continuity of operations or similar plans. Few were conducting regular backup operations and didn't have a written backup policy. Examples of these can be found on the Internet and adapted to fit organizations.
- Settings for common security tools and current patching for applications and operating systems.

As can be seen from the list of items all of the teams were required to address, the fact that few organizations had any of the items in place provided the students the opportunity to assess organizational specific needs and to provide recommendations in the final report. In several cases, enough time was left in the semester that students were able to assist organizations with the actual incorporation of some of these and in many respects the creation of an organizational cybersecurity program.

5. Results

A number of colleges and universities have courses which teach aspects of conducting cybersecurity testing and assessments. Some may also conduct these activities on organizations in their own communities. What is different about Project Xander is the number of organizations that were assessed and the intention of expanding this program to communities across the country in a coordinated fashion so experiences and lessons can be shared. Weekly Project Xander meetings were held to evaluate the progress, address issues that arose, and share ideas on ways to implement aspects of the assessments. Having the mentors participate in these meetings, and the eventual inclusion of members from other communities, separates Project Xander from other courses in which cybersecurity assessments and testing are conducted. Additionally, the MITRE Corporation has adopted this project as potentially a national program in which they could provide additional mentors for other universities and communities as well.

Feedback from the organizations, mentors, and students on the project were all very positive. Due to some issues that occurred during the semester, two organizations had to drop out. One was due to the organization folding and the other due to an actual cyberattack on the organization which had to be addressed.. Comments from students included:

> *Getting to have an actual experience in the field and interacting with real organizations to improve their cybersecurity was both very enjoyable and quite enlightening. The organization was very receptive to and appreciative of the things we proposed. Another thing this project was helpful for was forcing us to use less technical jargon to communicate information with people less versed in it. The mentor was extremely helpful and communicative. He provided an efficient communication pathway to the organization and also provided us with information and suggestions regarding how this scenario would play out in "real-life" -- JS*
>
> *This experience was very helpful and valuable, and I learned a lot from working real time with a small organization and being able to help them out with their security vulnerabilities. I would request something similar for future classes as this was a great learning opportunity. The organization gave us very positive and reinforcing feedback. They really appreciated our help, and they were very helpful with the whole process. The mentor was very helpful and was always attentive when we had any issues or problems or needed an answer to a question. – JG*
>
> *This was a tremendous experience as the team I was assigned to was able to meet with a real customer and work with them to develop a scope for the project. We heard directly from the customer, what their operations looked like and what their areas of concerns were. You*

> *read about these concerns and what organizations are up against where it comes to cyber, but it is a different experience altogether when those details come from your customer*. – NS

> *Project Xander was an excellent way for my peers and I to be able to further enhance our knowledge of cybersecurity in an effective method outside of a classroom setting. The real-world experience I was able to get by communicating and working with actual clients and security scenarios was able to set me up for future internships and potential consulting. Also, using industry practices and applying well known security frameworks was great to start having a more industry-focused mindset. I believe this was beneficial to the students by giving them a unique educational opportunity while also benefiting the organizations by allowing them to help strengthen their security posture.* AN

A comment from one of the mentors who provided feedback and included some additional factors follows:

> *I had no concerns with the students knowing the content. While we talked through things like checklists, questions, and assessment material, I found it beneficial to them to take time together to discuss client engagement and professionalism – NDAs and protocols to protect client information, appropriate attire and backgrounds in a virtual setting, and the way a meeting is formatted and run with goals, objectives, and outcomes. They picked up on it all, so in that regard, SUCCESS!*

How much the project helped the organizations is also obviously a good measure of the value of Project Xander. Without revealing the name of the organization so as to not encourage anybody from attempting to test their security, the following is a statement from one of the organizations that participated in the project:

> *Our small nonprofit benefited immensely in the process, dialogues and final report provided by the Project Xander Team. While we had a good sense of a cybersecurity posture we should have, the students asked the right questions about our organization that brought about new measures, training and policies we should implement. The final report was industry-quality, thorough and well written. The team was a delight to work with, especially watching the emergence of their respective student's leadership skills. Each member was respectful, courteous and professional. Their work was a harbinger of success for each of their respective careers. I highly recommend Project Xander for other nonprofits and faith-based organizations. They will learn about cybersecurity and how to protect their critical data and personal information.* – CT

The results from the assessments were fairly consistent across the organizations. Few of the organizations had any training or awareness programs, almost no written cybersecurity-related policies had been created, there were no plans for continuity of operations and only a few organizations were creating backup copies of important information on a regular basis. The students were able to provide hands-on assistance to the organizations to help them introduce each of these elements into an organizational cybersecurity program.

The original plan was to provide more assistance to the organizations after the conclusion of the assessment portion of the project but a late start in finalizing the organizations caused the assessments to be delayed resulting in less time to conduct assistance and also delaying the hoped-for technical portion of the project (e.g. penetration testing, simulated phishing attempts, and rogue wireless access point scanning). The more technical aspects were moved to the next semester. Only a few of the organizations felt ready to have a penetration test conducted. They wanted to have more time to implement the recommendations, especially those related to patching of applications and operating systems and ensuring security devices were correctly configured. Since not all of the students continued the next semester in the follow-on Cyber Operations course, new teams were created though an attempt to maintain the same team members for organizations was made. The Cyber Operations course had a lower enrollment so the fact some of the organizations dropped out after the initial assessment because they didn't feel prepared to continue worked out well.

As was done in class for the initial assessment piece, the students needed some experience with the sort of things they would do for a penetration test before they attempted to conduct the test on an organization. Consequently, a lab environment was provided along with an assigned lab for the students to gain experience with using normal penetration testing tools. Public domain tools were used for this lab.

One other thing that should be mentioned were the arrangements made to maintain the privacy and security of information related to the assessments. The MITRE Corporation provided access to a secure email and file storage environment for the duration of the assessment.

Students were instructed to NOT keep a copy of any of the assessment information on their own computers but to instead utilize the environment provided by MITRE. This not only again emphasized to the students the importance of maintaining the security and privacy of security-sensitive information, but it also provided assurance to the organizations involved that their information was being safeguarded and limited the possibility that copies of the assessments would be lost or released after the course was over.

6. Future of the Project

Project Xander was considered a success from all those who participated in the project – organizations, mentors, students, and the faculty members for the courses. It was beneficial for all participants and addressed a sector of the community which historically did not have robust (or any) cybersecurity programs and who also did not have the resources to contract with a vendor or hire cybersecurity professionals to implement a program. For smaller communities this could also be extended to local government and critical infrastructure organizations as well. The goal is to continue to operate the project and to assist other nonprofit and faith-based organizations in the community. In the 2022-2023 academic year two additional courses will be incorporated into the overall project.

The need to have an entity the target organizations can communicate with on a periodic basis to receive assistance for their ongoing cybersecurity programs was identified at the conclusion of the assessments. Discussions have been held as to how this might be accomplished. The students were interested in providing continued assistance as they felt it provided them excellent experience that would prove valuable upon graduation – not to mention experience beyond lab assignments that could be listed on their resumes. The idea being explored is to possibly have student-led organizations such as student chapters of professional organizations such as the ACM, W-ACM, or AFCEA staff a help desk that could provide assistance on an as-requested basis. Other organizations such as the student Computer Security Association also would be a prime candidate for helping provide this service. There are a lot of issues that need to be worked out before something like this is established including working out potential legal documentation to hold the university and students not responsible for any security incidents that might occur subsequent to recommendations that the students might make. Discussions continue on how best to add this level of assistance to Project Xander.

The major change in the future of Project Xander is the expansion of the project to other universities. This was a goal of the project from the start. Now that the efforts were shown to be beneficial for all individuals involved, the project will be expanded to other communities staring in the Fall of 2022. Four other communities including some in other states are in discussions for how to implement the project in their areas including one independent school district who wishes to explore the possibility of having high school students conduct similar activities. For the other communities, both two- and four-year institutions are the targets to provide the student assistance. Since the assessments for Project Xander were conducted while the university was still not holding on-campus classes due to Covid-19, the assessments and meetings were all conducted online. This did not prove to be an issue, though it did limit any physical security assessments, and a further expansion of the project will be to look at how schools in one community might be able to offer similar services to organizations in communities without a college or university.

7. References

DHS/CISA, The Department of Homeland Security/Cybersecurity and Infrastructure Security Agency, “Resources for Academia”, accessed 9/10/2022 at https://www.cisa.gov/uscert/resources/academia

Maimone-Medwick, J., and Tassel, A. (2022). “Nonprofit Organizations and Data Security Incidents – How to Manage and Respond”, April 7, 2022, Downloaded 14 June 2022 from https://www.jdsupra.com/legalnews/nonprofit-organizations-and-data-9788137/

NCSC, National Cyber Security Centre, UK, “The Problems with Patching”, accessed 9/10/2022 at https://www.ncsc.gov.uk/blog-post/the-problems-with-patching

Seda, P., Vykopal, J., Svabensky, V., and Celdea, P., “Reinforcing Cybersecurity Hands-on Training with Adaptive Learning”, Proceedings of the 51st IEEE Frontiers in Education Conference (FIE ’21). Lincoln, Nebraska, Downloaded 9/10/2022 from: https://arxiv.org/pdf/2201.01574.pdf

Shavell, R. (2021). “It’s time for NGOs and nonprofits to tighten their cybersecurity standards”. Downloaded 8 June 2022 from https://philanthropynewsdigest.org/-features/the-sustainable-nonprofit/it-s-time-for-ngos-and-nonprofits-to-tighten-their-cybersecurity-standards

Vojinovic, I. (2022). “More Than 70 Cybercrime Statistics – A $6 Trillion Problem”. Downloaded 8 June 2022, https://dataprot.net/statistics/cybercrime-statistics/