

Cybersecurity Internship at the Earth Viability Center

Date: August 9, 2026

Name: John Monrouzeau

Employer: Dr. Hans-Peter Plag

Company: Earth Viability Center (EVC) / Place4Us

Class: CYSE368

Term: Summer 2026

Table of Contents

1. Introduction	2
2. Management Environment	4
3. Major Work Duties, Assignments, and Projects	5
4. Use of Cybersecurity Skills and Knowledge	7
5. Preparation Through the ODU Curriculum	8
6. Achievement of Internship Outcomes and Objectives	9
7. Most Motivating and Exciting Aspects	9
8. Most Discouraging Aspects	10
9. Most Challenging Aspects	10
10. Recommendations for Future Interns	11
11. Conclusion	11

1. Introduction

This Summer 2026 semester, I completed my internship with the Earth Viability Center (EVC), working primarily with Dr. Hans-Peter Plag. My internship involved a combination of cybersecurity research, assessment of the MyHouse concept associated with Place4Us, examination of cybersecurity issues involving Virtual Community Centers (VCCs), and research into methods for identifying images and videos created using generative artificial intelligence. My primary goal for the internship was to gain practical cybersecurity skills and develop a better understanding of how cybersecurity knowledge can be applied outside of a traditional classroom or security operations environment.

The Earth Viability Center is an organization focused on supporting the long-term viability of Earth and encouraging collaboration among individuals and organizations working toward a more desirable future. The organization was co-founded in 2020, and Dr. Hans-Peter Plag has been involved in leading the Earth Viability Center team developing Place4Us since 2021. Place4Us is a basically a social collaboration platform made to help virtual communities and evidence-based collaborations. The platform is very heavily surrounded on the created Virtual Community Centers that allow participants and organizations to communicate, collaborate, and organize events and activities.

The EVC is different from the usual commercial companies. Its work combines technology, environmental and social issues, scientific research, and community collaboration. This made the internship very interesting for me, especially from a cybersecurity perspective because the security of the technology could not be considered separately from the people using it. A platform designed to facilitate collaboration has to consider all of the usual pillars of

cybersecurity, those being confidentiality, integrity, availability, privacy, authentication, authorization, and the potential chance of misuse by its users.

I became interested in the internship because it gave me an opportunity to combine the things I learned from my time at Old Dominion University studying Cybersecurity with a project that involved an actual online platform that needed cybersecurity efforts. Instead of just testing a system that had already been completely designed for a cybersecurity laboratory, like the usual labs that I was given during class to practice counterintelligence. I was able to actually look at security considerations in a professional and developing environment. This meant that I had to think about how users would interact with the system itself, what information could maybe become exposed, how access controls should operate, and what could possibly be at risk if a malicious or careless user attempted to take advantage of our weaknesses.

At the beginning of the internship, I was introduced to the the Place4Us platform, and the general goals of the projects assigned to me and my fellow cyber interns. One of my first impressions was that the internship was more independent than what I expected, especially after hearing what my cyber peers were doing at their own internships. During the internship, I had more responsibility for determining what information was relevant and how a problem should be handled. This meant that I had to become more comfortable with research, documentation, and explaining technical concerns in a way that could be understood by someone who was not necessarily approaching the problem from the same cybersecurity perspective, considering that not everyone working on the Place4Us platform was not necessarily very knowledgeable in cyberspace.

One of the most important objectives I hoped to accomplish was to be able to actually put my cybersecurity skills to use. My school coursework had of course given me a strong foundation, but I wanted to understand how cybersecurity professionals actually look at systems and identify security concerns in a much less controlled environment. A second objective was to improve my ability to identify and analyze cybersecurity risks. I wanted to be able to go beyond simply identifying that something was technically vulnerable and instead understand why the issue was an important one and how the issue could potentially be taken care of. A third objective I had was to develop my research and communication skills. Cybersecurity professionals quite often have to research unfamiliar technologies and communicate their findings to other people, which I was not very good at considering most of my classes at ODU were virtual. The internship gave me the opportunity to research subjects that I had not previously studied in depth, particularly methods for identifying AI-generated images and videos, and sharing my findings with my peers. A fourth objective I had set for myself that developed during the internship was to better understand the relationship between cybersecurity and the emerging or evolving technologies. Generative AI is completely changing how digital content is created, and this brings up new challenges for figuring out whether digital information is authentic. The internship gave me the opportunity to investigate this issue from a cybersecurity perspective.

Overall, my internship was an opportunity to connect cybersecurity with a broader range of technical and social problems. The experience showed me that cybersecurity is not limited to

firewalls, passwords, malware, or network monitoring. It also involves understanding how users engage with platforms, applications, information, privacy, emerging technologies, and the outcomes of specific design decisions.

2. Management Environment

The management environment of the internship was different from the highly structured management environments that exist in many larger organizations that some of my friends or people online would tell stories of their experience about. The Earth Viability Center is a pretty small nonprofit organization whose work involves collaboration among people with different areas of expertise. The organization has a consortium-oriented approach, and its work involves scientific, technological, environmental, and social issues. The EVC's website describes a consortium structure in which participating organizations can contribute to the organization's direction and decision-making. My primary supervision came through Dr. Hans-Peter Plag. His background includes scientific research, sustainability, geophysics, Earth system science, and the main developer of the Place4Us platform, considering he is the founder.

The management environment required a significant amount of independence, especially since the internship was completely virtual. Rather than receiving constant step-by-step instructions, I was generally given a project or research objective and then expected to investigate the subject. I didn't really mind this independence, because not only is it expected in a proper and professional environment, but I also found that I worked a lot better on my own. The supervision worked out for me because I was able to work independently while still having someone there for me to provide direction when I needed it. This helped me to develop my own research and analytical skills without being completely isolated from someone to give me guidance. When I had any issues that required clarification, I could discuss the problem with my peers or Dr. Hans-Peter and determine how to proceed.

Another important characteristic of the management environment was the interdisciplinary nature of the work. Cybersecurity was only one component of the larger projects. The work also involved social collaboration, environmental concerns, artificial intelligence, software design, and user behavior. This required me to consider cybersecurity from perspectives beyond the technical aspects that are normally emphasized in cybersecurity courses.

The management environment also reinforced the importance of communication. A cybersecurity finding is only useful if the people responsible for a system can understand the actual finding, while also determining and acting on what actions should be taken. Because of that, I had to think about how to explain technical issues clearly instead of just using the regular cybersecurity terminology.

Overall, I found the management environment effective for an internship because it encouraged independence while still providing direction. It also helped me develop a better understanding of how cybersecurity work can function in a small organization where employees and contributors may perform multiple types of work.

3. Work Duties, Assignments, and Projects

My internship consisted of quite a few major projects. Although these projects were different from each other, they were connected by a common goal: understanding and improving the security and reliability of digital information and online collaboration.

MyHouse Cybersecurity Assessment

One of my major projects involved assessing the cybersecurity of the MyHouse concept. MyHouse is associated with the Place4Us environment and is designed as a user's unique digital home. It can contain different rooms and areas, and users can configure access for different categories of people. A platform with this type of structure brings up quite a few important security questions for me. For example, users need to be able to control who can access information. The system also needs to make sure that one user cannot access another user's private information just by changing a URL or manipulating an identifier of sorts.

One of the issues I considered was predictable user identification and URL enumeration. If user IDs or URLs can be predicted, an unauthorized individual might be able to locate information belonging to another user. This is an important security concern because a system should not assume that information is secure merely because a user does not know the URL. I also examined access control and authorization. Authentication determines who a user is, while authorization determines what that user is allowed to access. A secure system needs both. Even if a user is successfully authenticated, that does not mean the user should automatically have access to every resource within the platform.

The MyHouse concept also raise a couple privacy concerns. Because users could potentially store or share information within different areas of the platform, the system needed to make sure that information is visible only to the people it was intended for. Privacy issues can become especially important when the system allows users to share rooms, files, or other resources with selected people or communities.

I also considered issues related to soft links, file-system management, and scalability. A system that grows over time needs to maintain accurate relationships between users, files, rooms, and permissions. Poorly managed file relationships can create security or reliability problems.

This project was necessary to the organization because cybersecurity problems identified before a system becomes more widely used can potentially be addressed before they become major vulnerabilities. Identifying problems early can be significantly easier and less expensive than attempting to fix them after a platform has accumulated a large number of users and large amounts of information.

Cybersecurity of Virtual Community Centers

Another area of my internship involved examining cybersecurity considerations for Virtual Community Centers. Place4Us is designed around VCCs, which provide communities with digital spaces for communication and collaboration. The platform includes features such as messaging, blogs, discussion areas, administration areas, and other tools for community interaction.

This created another set of cybersecurity questions. A VCC can contain many different users with different roles and permissions. Administrators might need access to information that average users should definitely not be able to access. At the same time, users need enough access to perform proper activities.

I considered the importance of authorization, account management, privacy, and protection of user-generated content. Because VCCs are designed to encourage communication, there is also a need to consider inappropriate content, malicious links, impersonation, and other forms of abuse. A legitimate user with inappropriate permissions may unintentionally or intentionally expose information.

This project helped me understand that cybersecurity is closely connected to application design. Security controls have to be integrated into the way the application operates rather than added only after the system has been created.

Generative AI Image and Video Research

Another major part of my internship involved researching ways to identify images and videos created with generative AI tools. This was very interesting for me because generative AI makes it very hard to determine whether digital media is authentic, especially with how recent of a technological advancement it is. A person can now create highly realistic images, modify photographs, generate synthetic people, or create videos that appear authentic. This creates cybersecurity concerns because digital media can be used for impersonation, misinformation, social engineering, fraud, and manipulation.

I investigated methods that could potentially help distinguish AI-generated content from authentic content. This required examining the limitations of detection methods as well as their potential uses. One important lesson was that AI detection is not a simple problem. A detector may identify characteristics associated with a particular generation method, but AI models continue to improve. Content can also be edited after it is generated, making detection more difficult.

This project was necessary because organizations should very often need to evaluate the authenticity of digital information. Cybersecurity professionals cannot assume that a photograph or video is genuine just because of how realistic it looks.

Research and Documentation

In addition to the specific projects, research and documentation were important parts of my internship. I had to locate information, evaluate it, organize findings, and explain conclusions, while also citing my sources.

Research is an important cybersecurity skill because cybersecurity changes continuously. A professional cannot expect to already know everything about every technology or vulnerability, especially because of how much the cyberspace changes and newer strategies and technologies are implemented. Instead, cybersecurity professionals need to know how to find reliable information and determine how it applies to a specific situation.

4. Cybersecurity Skills and Knowledge

The internship allowed me to use cybersecurity skills that I had already developed through my education while also requiring me to learn new skills. Before beginning the internship, I had experience with fundamental cybersecurity concepts such as the CIA triad, access control, authentication, authorization, network security, vulnerability assessment, risk management, Linux, Nmap, Wireshark, and other cybersecurity tools and concepts.

These skills helped me recognize security concerns during the MyHouse assessment. For example, understanding authorization helped me recognize why it was important to determine whether users could access resources that they were not supposed to access. The concept of least privilege was also relevant. Users should receive only the access necessary to perform their legitimate activities. This becomes particularly important in a platform where users can interact with different rooms, communities, files, and resources.

Risk management was something I got much better at understanding during my internship, because before this internship I thought it was just a plan with set, predetermined responses that needed to be done. But I learned that finding a vulnerability is only part of the job. You also gotta think about what could happen if someone used that vulnerability within the system you are protecting, and you also have to be mindful of how it could affect the system or its users. Working on MyHouse also showed me that security should be considered when a system is being designed, not just added later. Things like user access, files, and permissions need to be planned out so that users cannot access things they aren't allowed to access.

The generative AI research also gave me a different view of cybersecurity. Through this internship, I started to see that digital content can also create security problems, especially when AI can be used to create realistic images and videos. This could be used for scams, fake information, phishing, or impersonation. I also became better at researching unfamiliar topics since some of the work was new to me. Overall, the internship showed me that cybersecurity requires learning new things as technology continues to change.

5. How the ODU Curriculum Prepared Me

My coursework at Old Dominion University most certainly prepared me for the internship in several important ways, and helped me gain a strong understanding of cybersecurity. My cybersecurity coursework taught me how to think about vulnerabilities and threats. The labs that I was assigned in my classes used tools such as Nmap and Metasploit, which demonstrated how security professionals can identify and look over vulnerabilities. The same mindset that I had for my in school labs were the same ones that I felt were useful at my internship: understand how a system works, identify potential weaknesses, determine the consequences, and consider appropriate protections.

Risk management coursework was particularly relevant. The internship required me to think about the potential consequences of security weaknesses instead of only identifying technical problems. The CIA triad was another concept that appeared throughout the internship. Confidentiality was relevant when considering who should have access to information. Integrity was relevant when considering whether information or digital media could be manipulated. Availability was relevant because users need reliable access to the services provided by the platform. Access control concepts were especially important to the MyHouse and VCC projects. The difference between authentication and authorization became more practical during the internship. It was not enough to ask whether a person could log into the system. I also needed to consider if the person should be able to access a particular room, file, or resource.

The internship also strengthened my understanding of concepts involving social engineering and human behavior. A cybersecurity professional has to understand that people are part of the security environment. Users can make mistakes, fall for deceptive content, share information incorrectly, or misuse legitimate access. At the same time, the internship revealed areas that I had not fully encountered in my coursework. The research involving generative AI was one example. While AI is becoming increasingly relevant to cybersecurity, identifying AI-generated media was not a major component of many of my traditional cybersecurity labs.

The internship most certainly complemented my ODU education. School gave me the technical foundation, while the internship showed me how those concepts could be applied to less structured and more ambiguous problems. Another difference was the amount of independent research required. Academic assignments normally provide a defined question. During the internship, I sometimes had to determine what questions should be asked in the first place. This experience helped me understand the value of my ODU curriculum while also showing me areas where I can continue developing.

6. Outcomes and Objectives

My primary internship goal was to gain cybersecurity skills. Overall, I believe this goal was fulfilled. The first objective was to gain practical experience applying cybersecurity knowledge. The MyHouse assessment allowed me to apply concepts such as access control, authorization, privacy, vulnerability identification, and risk analysis to a real platform. This was different from a classroom exercise because the system was not simply an artificial example created for an assignment. The second objective was to improve my ability to analyze cybersecurity risks. This goal was fulfilled through my work examining potential weaknesses in MyHouse and Place4Us. I learned that identifying a problem is not enough. I needed to consider how the issue could affect users and the organization. The third objective was to improve my overall research skills. This goal of mine was done through the research involving generative AI detection. I had to investigate technologies and approaches that were outside my existing area of expertise. The fourth objective was to gain a better understanding of emerging cybersecurity issues. The AI research strongly contributed to this objective. Generative AI has introduced new opportunities as well as new threats, and understanding these developments will be important for future cybersecurity professionals.

The internship also helped me become more comfortable with uncertainty. As obvious as it may sound, not every problem will have a clear answer, or even an answer at all. Sometimes the whole point of research is to just be more aware of a potential concern or threat later down the line, instead of just immediately working on a solution. This was an important learning experience for me because professional cybersecurity work often involves incomplete information, and putting together puzzles using few pieces. Security professionals have to make reasonable assessments based on the information available to them.

Overall, the internship fulfilled my main goal of gaining cybersecurity skills while also giving me a better understanding of how those skills can be applied in a professional environment.

7. Most Exciting and/or Motivating Aspects

I have to say that from all of the good things I gained from this internship, the most important positive thing to me was the fact that I was working on actual real world work problems, and applying my knowledge and skills towards something proper. The MyHouse assignment, for example, was very fun to me because of how fresh yet important of a concept it was to the future of the platform. I was looking at an actual platform concept and thinking about how it could be attacked or misused.

I also found the generative AI research I had to do exciting because it represents a rapidly developing area of technology. AI is changing quickly, and cybersecurity professionals will have to adapt to those changes. Another motivating aspect was the independence of the internship. Being trusted to research a problem and develop findings made the work feel more like professional experience than a traditional school assignment. The interdisciplinary nature of the organization was also motivating. Cybersecurity was connected to environmental issues,

social collaboration, technology, and community organization. This showed me that cybersecurity can have applications in many different fields.

Overall, the internship further proved to me that a career in cybersecurity is absolutely what I want to pursue in life. I enjoy looking at and analyzing systems, figuring out any weaknesses, and doing my own research on issues that others are unfamiliar with.

8. Most Discouraging Aspects

Despite it all, I still did have some things that demotivated me quite often. One of those things was the attendance of my peers. Because the internship was unpaid, a lot of the other interns would rarely join in on the 2 weekly meetings we had. They did their work, yes, but there weren't many times where we could all just look over common issues or discuss concerns for the site and whatnot. In fact, I found myself being the only one in a call with our boss, Dr. Hans-Peter, quite often.

Another discouraging thing was that the internship itself was completely online. So not only were my fellow interns not participating or communicating too often, but I was also struggling to connect with them and socialize. There were even times where I would also want to slack off and not commit to my responsibilities because of this. But I suppose this is something that a lot of cybersecurity professionals must face eventually, considering a lot of jobs are virtual or hybrid.

9. Most Challenging Aspects

One challenge I had was understanding the system from the perspective of different users. A security analyst has to think about what a normal user should be able to do as well as what a malicious user might attempt to do, but I have never had to really emphasize or focus on what random users on a platform are doing, so it was something I had to adapt to.

Communication was another thing. When issues were found, I had to figure out a way to make it sound clear and understandable to people that weren't super familiar with what exactly was being spoken about, as well as the potential solutions for the issues.

The final challenge I really had, as mentioned before, was working with my fellow interns. It felt like everyone's schedule was against each other's at several times unfortunately, and of course that just tends to happen, but it was very often. I am hoping that for future interns, it's very different.

10. Recommendations for Future Interns

There are many things I could tell the future interns for this same internship role, but the biggest and most important thing is to be ready to work on your own. This is not the usual internship. The tasks assigned to you will be your responsibility, and you must do your own research and put it to the test the best you can.

Future interns should also have a strong foundation in cybersecurity concepts. They should understand authentication, authorization, access control, confidentiality, integrity, availability, vulnerabilities, threats, risk, etc etc. Basic networking knowledge is also useful. Understanding how systems communicate makes it easier to identify potential security concerns. Java scripting and command-line experience can also be beneficial to access the testing site and make changes as needed. Cybersecurity students should be comfortable navigating technical environments and researching problems using the same tools used throughout our coursework.

Another recommendation is to develop strong research skills before beginning the internship. An intern will not know everything required for every project. The ability to locate reliable information and understand unfamiliar technology is therefore extremely important.

Lastly, interns should be ready to adapt and overcome the usual cybersecurity stuff that we are taught in class. Technologies are always evolving and changing up the cyberspace, especially now that AI is playing a heavy role all around the world.

11. Conclusion

My internship with the Earth Viability Center was an experience that I am very grateful for. Originally, I was meant to just take the alternative course because I couldn't land an internship after months of searching. Luckily I was able to get this opportunity, and now I am leaving much more knowledgeable than how I started. Taking the things I had learned here at Old Dominion University, like risk assessments, CIA triad, and access control, and being able to actually apply it all to a real-world issue was very fun.

One of my biggest things that I took note of from the internship is that cybersecurity requires a lot more than just knowing how to use security tools and strategies. I had to research a lot of things on my own, think about how different users could interact with our system, and explain security concerns to people who may not have the same cybersecurity background as me. The independence of the internship also helped me become more comfortable with figuring things out on my own rather than always having someone give me the exact steps to follow.

This experience will definitely have its impact on me for several years to come. I want to keep building my technical knowledge while also getting better at researching and analyzing problems from different perspectives. This internship also confirmed for me that cybersecurity is the career I want to commit to in life. I enjoyed finding weaknesses, researching topics, and

figuring out how a system can become more secure. I know there is still a lot for me to learn, but this internship gave me real world experience and a better idea of the goals I have for my future self.