**Jordan Davis**

**CYSE 368**

**Spring 2026**

**Professor Teresa Duvall**

**TA Joshua Russell**

**Virginia Air and Space Science Center**

**Interview / Reflection #2**

**Introduction**

The following is an interview I conducted with my direct supervisor at the Virginia Air and Space Science Center, Kim Ward. I created a list of six questions that relate directly to her work experience as the coordinator of volunteers, interns, and docents, and each question will be followed by a paragraph written reflecting on the answer and its possible ties to the field of Cybersecurity.

**Interview**

- How are responsibilities divided among staff, interns, and volunteers? **Staff are paid employees at the center. Volunteers are unpaid. Volunteers include docent, and high school level volunteers. Interns are typically a paid position and we give them more responsibility, but fundamentally the distribution of tasks include a hierarchy where the paid staff are more of the Frontline supervisors of the interns docents and volunteers, and they - meaning the volunteers and interns - need to follow strict guidelines in order to be able to work with the public. So, I'm trying to - besides the supervisor position - for the paid employees volunteers and interns actually interact with the guest in a more hands-on fashion and are more of a front line to guest services, so training in the soft skills is important so that they interact with the guest in a positive manner**.

Kim indicated that the supervisory staff are mainly responsible for ensuring that protocol is upheld and safety is prioritized by the lower level staff and volunteers. The volunteers and interns are more focused on public interaction and supporting the proper functioning of the educational exhibits. This can relate to cybersecurity when we look at the relationship between IT staff and end users: IT Staff set up the backend systems so that the end users can utilize the proper tools without having too much access to the system or posing unnecessary risk to the system itself. There is also overlap between the public relation training and training that employees would receive in a cybersecurity setting, as both utilize employee education as a method of mitigating risk to either the guests or to the systems themselves.

- What kind of training do interns receive before starting **For interns, Docents, and volunteers they go through a 30 minute orientation with an hour long, hands-on training and then a shadowing program where they shadow experienced volunteers until they feel comfortable going solo**

This tracks with the training that I personally received at my internship placement. My first day consisted of a tour of the facility, followed by a hands-on walkthrough of the different educational exhibit stations that I have the opportunity of running whenever I am volunteering. This relates to the field of cybersecurity because the end user is one of the most major security risks, whether it's through failure to follow proper procedure or whether an employee falls victim to a phishing attack. These scenarios are both mitigated by thorough training of employees, which is a common thread between the VASSC and cybersecurity as a whole.

- How do you ensure that volunteers follow proper procedures? **I ensure the volunteers follow proper procedures by monitoring their interaction with guests and spot checking them on occasion may include somewhat of an eavesdropping or pretending to be a guest situation where it's a role-play between how they would interact with a guest that maybe was not complying to our safety standards for example.**

This "eavesdropping" method is similar to the act of packet tracing in cybersecurity, as well as other digital forensic methods. It is common in cybersecurity to actively monitor accounts and actions taken by employees to discover and proactively mitigate threats. The other method, "pretending to be a guest" reminds me of penetration testing, where a company may hire an ethical hacker to attempt to breach their data systems, rather than waiting for a truly malicious hacker to exploit their security flaws.

- How do you enforce rules or protocols among a large group of visitors? **We typically greet large groups at the main entrance when they check in for their visit. Most large groups are chaperones by adults from the same organization and we require them to have a ratio of one adult per 10 students or children so they are internally monitoring themselves with their chaperones, but in addition when they arrive at the center, we tried to greet**

**them either by the docents, one of our staff members, or an educator who's running one of their programs and give them strict guidelines on what the schedule entails and proper museum protocols like no running for their safety and keep the volume down so that other guests can enjoy their experience in the event of an incident or in need to regulate a large group during the course of their visit, we rely on the docent and volunteers to kind of keep an eye on exhibits and guest behaviors, and give them the authorization to politely and respectfully with a smile. I'm trying to maintain the crowd and encourage proper safe practices with the guests and not necessarily scold them if something's being done that we don't approve of.**

These are examples of policies which can be used to determine the proper flow of guests through the facilities as well as the proper usage of certain rooms or devices. In cybersecurity, we have policies dictating the use of user accounts, software, and devices which are designed to prioritize safety and security of user data. Clearly, no matter the field, whether its public education or cybersecurity, policy is generally used in the protection of sensitive assets.

- Who gets notified of issues in the museum or its exhibits, and how many people are usually involved in fixing a problem? **Regarding an issue in the center, if it's a safety concern or potentially an injury, we immediately go to security and proper medical staff are identified and called on the scene. For**

**example, most recently an allergic reaction was witnessed in the center and a 911 was called immediately so we have protocols in place where security is alerted of everything and in the event medical intervention is needed we call 911. We also obviously have a great relationship with the police department in the city of Hampton, where they support us in different instances like a custody dispute, which we also had called last week. That being said, if a guest injures themselves on site and refuses medical intervention, we do have waivers that they have to sign before they can leave indicating that they won't follow up with legal action after the fact.**

This is an example of chain of command and incident response. In the museum, they prefer to delegate incident response to either their in-house security or to outside authorities. This is reminiscent of a company hiring an external cybersecurity firm, or a digital forensic team, in order to investigate a cybercrime. Obviously, mitigation happens mostly in-house, but incident response can involve external help as well.

- If you could improve one thing about the museum or its systems, what would it be? **I think one thing I would improve about the systems would possibly be more funding to hire more staff on a full-time basis so there's more continuity with communication. Most miscommunications occur in the center between departments that don't see each other frequently enough because they're part-time and it creates problems with guest relations that could've been prevented, had we just had adequate staff here every day of**

**the week we could also with more full-time staff have the center open seven days a week, whereas from the months in between Labor Day and September and Memorial Day in May, we are closed Monday and Tuesdays, but having a larger staff funding, we would be able to open seven days a week and therefore create a better product for our community as well.**

Kim's main points that she would like to see improved are increased funding and reduced downtime. This is a common thread in many fields, and especially so in cybersecurity. An increased budget can help to hire more professionals in the protection of assets, and the more professionals are supporting asset safety, the less downtime is likely to occur in company servers or devices.

**Conclusion**

Interviewing my supervisor and adapting her responses to relate to cybersecurity has been an interesting exercise in connecting two relatively separate niches. As I continue to work this internship, I will continue to identify connections between the public education sector and the cybersecurity sector. I believe that making these connections will not only broaden my knowledge in cybersecurity, but also hone my social skills through work experience and allow me to achieve a great career.