Patrick Bays

CYSE 368

ODU Spring 2026

Professor Teresa Duvall/TA Joshua Russell

ANVIL Systems Group, Inc.

Reflection #2

03/08/2026

Internship Reflection Paper

100 Hours

Working as a network/field engineer for 100 hours has given me knowledge into CMMC Level 2 file storage requirements, and the importance of backup systems. I was woken up on a Monday morning to find that the Synology NFS share that hosts all of our project files, documentation, and working documents had gone offline. I quickly showered, got dressed, and ran in with my coworker to diagnose the issue. We found the box offline – no rack-level power failure or anything obvious upon first glance, it seemed like it had just died. After pulling both power supply plugs, waiting for capacitors to discharge, and plugging them back in, the Synology booted up to life again. However, it was only accessible over the corporate network, on its second NIC – we let the Synology service do its mandated data scrubbing on unexpected power loss, and investigated why it couldn't be seen over our development network (two separate subnets, two separate NICs). We found that the switch that fed it our development network link had kicked the bucket, but we couldn't figure out what ended up happening to the power. We decided to place an order for a new Synology box assuming an internal power failure, and reconnected the machine back

onto our development network. We had no other choice than to keep this box online due to the fact that it's our only Synology system that has full volume encryption (FVE) as a service – its the only one that would be compliant under a CMMC Level 2 audit, which we anticipate happening at the end of Q2 this year. I then took initiative to setup a Synology diskstation (which is not compliant) as a temporary file backup of our live fileshare server, to minimize data loss in the event this happens again. Other than that event, I continued my STIG efforts for blue team remediation. Last week, some of our equipment at a remote site was damaged. Our CEO designated us to prepare emergency communications boxes in the event that comms couldn't be restored through traditional means. Our boxes contain an LTE modem, a SATCOM modem, and a layer 3 switch to route traffic in the event of loss of signal. Our 3-man network team worked like crazy, salvaging older boxes from previous installations, testing previously yellow-tagged equipment for basic functionality, and conducting failover tests to make sure they all behaved properly. It was a real "drop everything" moment for a few days, but we worked together in tandem with our other field engineers (testing devices) and electrical engineers (making power cables) to make it happen.

The value of maintaining proper backup systems and employee cohesion in a time of crisis are the most important things I've learned. A great part of being part of a small company (ANVIL only has 26 employees), is that our cohesion as coworkers is essentially lock-step with one another. No emails to supervisors asking if we can pull a specific number of people for a task, no crazy amount of red tape to make something happen, just pure raw communication. It was incredible experience heading an emergency effort like this, from delegating tasks to others not in my team to working within my team to get each task done efficiently. In regards to the Synology failure situation, it was also great to have a like-

minded coworker with me, especially one who shares similar problem-solving methods. It also highlighted that, even in transitory periods where we're acquiring and installing new hardware often, failures do happen, and it's not worth gambling while having no lines of defense.

In addition to work… My software engineering course still took up the bulk of my time, I also had midterms (yay…) so a lot of my spare time was spent studying for those. I didn't really get anything else done that was technical, I mainly just spent what little free time I had playing video games with friends and checking up on scan progress from home using my work VPNs.

Overall, the first 100 hours have been quite the whirlwind. Diving into incident response (especially trying to resolve incidents that happen hundreds, if not thousands of miles away) was a real challenge. The Synology failure event hammered home to me how important backups are and why we need to be prepared for anything at all times. The emergency comms boxes incident was also a crazy experience, but it showed me what our team can accomplish when we work together under pressure. Being part of such a small company means that everyone has their own weight to pull, and seeing that level of cross-team teamwork firsthand was awesome. It's still as challenging as ever to find time to be prepared for my classes and work, but this semester has been a test of my time management skills (as you know…). This experience has definitely provided even more perspective into what cybersecurity and networking work is really like (even beyond the technical aspects), and I feel very lucky to be working with a like-minded team.