

Mathieu Crosby

CYSE 368

Individual Reflection

Over the course of my experience in CYSE 368 I watched the abstract language of my cybersecurity courses turn into lived experience. From the opening week, expert mentor John Costanzo, flanked at key moments by Valor Cybersecurity's Greg Tomchick, and tightly focused guest lectures from Dr. Baaki placed our student team inside an authentic consulting workflow, testing every concept we thought we already understood. As spring unfolded, I moved from note-taker to practitioner: first conducting field assessments under supervision, then, by the 100-hour mark, interviewing JenDore's founder with my assigned team. In the final sprint I took the role of the design-lead mantle, shaping a minimalist slide deck and branded incident-response template that carried our findings from classroom to client boardroom. Which follows is a narrative reflection on what went right, what went wrong, and how the experience is recalibrating both my remaining time at Old Dominion University and my professional trajectory.

What went right first and foremost was the quality of mentorship. Greg's weekly de-briefs translated textbook controls into the messy textures of a real e-commerce stack, while Dr. Baaki's sessions on threat modeling expanded our analytic vocabulary beyond compliance checklists. Guided autonomy was another win; being trusted to lead client dialogue without a senior consultant in the room crystallized the confidence leap from student to junior analyst. Finally, the team's role clarity paid dividends—our tech lead validated Valor's Cybersecurity checklist scores while I iterated slide aesthetics—so we delivered the NIST-aligned risk assessment and an Incident Response Plan on schedule.

Many things went wrong along the way. A calendar mishap in week five erased a scheduled client check-in, forcing us to compress two weeks of discovery into four frantic days and reshuffle our ideas. Mid-semester the client launched a new merchandise line; several risk scenarios we had already drafted were suddenly obsolete. I also burned hours cycling through six visual themes before we locked a universal branding palette—time that better-defined design requirements up front would have saved.

These stumbles carried hard-earned lessons that map directly onto our Memorandum of Agreement objectives. Our charge to “apply classroom theory to a real cyber-risk assessment” was met whenever I watched an abstract control become a concrete change request for JenDore; the takeaway is that understanding the “why” behind a control accelerates choosing the right “how”. Producing client-ready documentation underscored the value of version control: disciplined peer-review loops shielded us from eleventh-hour edits. The objective of professional communication blossomed most vividly in that solo interview, where I learned that listening often reveals vulnerabilities faster than technical scans. Our commitment to ethical, team-based decision-making was tested—and proven—during spirited debates over risk-rating thresholds; data-backed dissent raised the final quality .

Among the most motivating moments, nothing matched the live client presentation. Compressing eight weeks of analysis into twenty crisp minutes, then watching JenDore’s founder nod through each slide, electrified the room. Close behind was the email, forty-eight hours later, confirming multi-factor authentication had been enabled across all admin accounts—a reminder that well-framed guidance moves people to act. The flip side was the grind of time management. A cryptography mid-term collided with our disaster-recovery workshop, and more than once I felt my attention fray while toggling between slide layout . The

rapidly shifting Shopify API also forced us to re-validate controls, teaching me that cyber-defenses are never “done.”

Future interns can soften those edges by arriving proactive. Send meeting agendas a day in advance; ambiguity shrinks when expectations are on paper. Master your tools—Canva, PowerPoint, Git—before the semester accelerates, and treat every Slack thread as source material for the final report. A quick skim of NIST SP 800-30 and the free Shopify Partner Academy module will anchor the technical baseline from day one. As for the course itself, I would preserve the real-client model that makes the work matter, but introduce branded slide templates in week two and add a one-hour version-control boot camp; both tweaks would have cut our design churn in half.

Stepping back, three insights frame my takeaway. First, empirical humility: even a “simple” online merch store hides a labyrinth of third-party apps and unpatched corners. Second, the compounding value of structured communication: a clear question today saves hours of rework tomorrow. Third, the tangible thrill of impact: when JenDore flipped the MFA switch, coursework morphed into client security. Those lessons will steer my ODU path toward electives in cloud security architecture and a senior capstone on small-business cyber resilience. Professionally, the project nudged me from generic analyst ambitions toward consultancy, where technical rigor and client storytelling intersect. In short, serving as JenDore’s design lead at the close of the internship transformed cybersecurity from an academic pursuit into a human-centered service I now intend to chase full-time.