CYSE 368 Internship Final Paper

Fall 2025

Brandon Sutton

Toano Contractors

Cybersecurity Intern

December 1, 2025

Table of Contents

I Introduction

Internships play a crucial role in shaping a student's professional identity, especially in a field as dynamic and rapidly evolving as cybersecurity. Classroom learning provides a strong theoretical foundation, but true competence comes from applying that knowledge in real situations where systems, people, and business processes intersect. My internship with Toano Contractors gave me a firsthand opportunity to experience those intersections. Although the company is not traditionally associated with hightech environments, the modern construction industry relies heavily on digital systems, mobile devices, and secure workflows. This reality made my experience far more impactful than I initially expected.

During my 150 hours at Toano Contractors, I learned how cybersecurity principles apply not in hypothetical scenarios but in daily operations where decisions must be practical, efficient, and tailored to the needs of staff who are not cybersecurity professionals. Throughout the internship, I worked on tasks involving device management, workstation setup, troubleshooting, account administration, cybersecurity awareness, and mobile data support. Each task expanded my understanding of how technology functions in support of real business objectives.

This paper provides a comprehensive reflection on the experience, including the structure of the company, the responsibilities I held, the challenges I faced, and the broader cybersecurity lessons I gained. It also includes additional sections that examine the tools I worked with, the workflow of IT operations in a construction environment, my personal growth, and the influence this internship had on my future career plans. The final result is a detailed account of how this internship shaped not only my skills but also my confidence and professional goals within the cybersecurity field.

II. Overview of Toano Contractors and Its Technology Environment

Toano Contractors is a construction company that manages multiple projects, coordinates field and office staff, and maintains detailed documentation for each stage of its operations. Like many construction organizations today, Toano Contractors uses an extensive blend of digital tools to support communication, time tracking, project updates, equipment logs, and customer information. Even though the core business revolves around physical work such as building, installations, and site inspections, the backbone of daily coordination is technological.

The company's technology environment includes desktop computers for office staff, mobile devices such as Samsung tablets for field workers, cloud storage systems for documentation, project management platforms, and communication tools for sharing updates quickly across teams. Most of this technology is interconnected, meaning employees rely on synchronized systems to upload photographs, log work progress, and check schedules or updated instructions.

The reliance on mobile technology is particularly important because employees frequently work on different job sites and must update information in real time. These devices support everything from digital blueprints to timestamped project notes, and any malfunction or security issue can slow down a project significantly. This dependency highlights why cybersecurity is not exclusive to large corporations but essential for all businesses operating in a digital ecosystem.

The company's environment also includes several challenges typical of small to medium-sized businesses: limited dedicated IT staffing, mixed experience levels among device users, and a need for efficient systems that do not interrupt the fast-paced nature of construction work. These challenges made my role as a cybersecurity intern especially meaningful, as I learned firsthand how cybersecurity must be balanced with usability and workflow demands.

III. Role and Expectations of a Cybersecurity Intern

As a cybersecurity intern, my role involved a mixture of IT support, device management, security awareness tasks, troubleshooting responsibilities, and active participation in maintaining reliable systems. While my academic background prepared me with foundational knowledge in networking, threats, authentication, and system administration, this internship taught me how to apply these concepts in ways that genuinely mattered to the company's operations.

On my first day, I was introduced to the systems the company relied on and received a walkthrough of the most common technical issues employees faced. These initial expectations emphasized reliability, communication skills, and problem solving over purely theoretical cybersecurity concepts. I quickly learned that being a cybersecurity intern in this environment required adaptability and the ability to think through practical solutions that benefited end users.

My supervisors expected me to handle tasks independently whenever possible, seek clarification when necessary, and maintain awareness of both security and efficiency. The role demanded that I support employees who had varying levels of familiarity with technology, which required patience and the ability to explain concepts clearly. This was especially important when helping employees understand why certain cybersecurity practices were necessary, even if they added extra steps to their routines.

Overall, the expectations of the internship aligned closely with what a real cybersecurity support role looks like in a small business: not just protecting systems, but helping people use those systems confidently and securely.

IV. Daily Operations and Workflow Integration

A typical day during my internship involved supporting both office staff and field employees. I often began by checking for any reports of issues from the previous day, such as malfunctioning tablets, computer slowdowns, synchronization errors, or software notifications. Some mornings required immediate troubleshooting if a device essential for jobsite reporting was not functioning correctly.

Many tasks involved configuring settings, managing user accounts, checking system updates, and testing devices to ensure they were secure and operational. I frequently assisted the office manager, field supervisors, and project leads by preparing tablets or workstations they would

need throughout the day. When returning employees reported problems, I gathered details about the symptoms, assessed the device, and followed a systematic approach to identify the root cause.

This workflow helped me understand the daily rhythm of an IT environment within a nontechnical industry. Instead of predictable schedules, tasks often arose unexpectedly and required immediate attention. I learned to prioritize based on urgency rather than chronological order. For example, if a tablet malfunctioned on a job site, resolving that issue took priority because it affected realtime reporting.

Participating in daily operations helped me understand how technology supports the company's workflow, builds efficiency, and impacts employee productivity.

V. Core Technical Responsibilities

One of the most significant parts of my internship involved handson technical responsibilities that strengthened my understanding of system administration, device management, and basic cybersecurity practices. I handled tasks such as diagnosing slow systems, reinstalling software, creating and configuring user profiles, and ensuring that devices operated under secure settings.

A recurring responsibility was checking for system updates. Keeping operating systems, drivers, and software up to date is a key cybersecurity practice because outdated systems can contain vulnerabilities. In many cases, updates also resolved performance issues or provided features that employees relied on.

Another core task was device configuration. When employees received new workstations or tablets, I was responsible for preparing the devices to function properly within the company's network. This involved applying standardized settings, configuring user environments, installing required software, and ensuring that security controls were enabled.

Troubleshooting was also a frequent part of my responsibilities. Employees often faced issues such as frozen applications, connectivity errors, login problems, or storage limitations. Each issue required patience and a structured approach to identify the cause. Through this process, I learned how to diagnose both hardware and software problems, test potential solutions, and restore devices to proper working condition.

These technical responsibilities not only helped keep the company operating smoothly but also strengthened my confidence in handling diverse technology systems.

VI. Working With Samsung Tablets and Field Data Systems

One of the most unique aspects of my internship was working closely with the Samsung tablets used by field employees. These devices served as the company's primary method for collecting project data, uploading photos, recording notes, and maintaining communication between job sites and the office. The reliance on these tablets made their proper functioning essential.

Throughout my internship, I worked on issues such as slow performance, storage management, syncing failures, and app crashes. One of the most common problems involved the tablets running out of storage due to the large number of photos taken at job sites. When this happened, the tablets became slow and sometimes failed to upload new data. To address this, I assisted employees in organizing media files, clearing unnecessary data, and syncing important information to the appropriate cloud folders.

Another recurring issue involved software updates. Some tablets had outdated applications that caused compatibility issues with the company's project management software, preventing uploads or freezing during use. I ensured that updates were completed properly and tested the devices afterward to confirm that the issue had been resolved.

Working with the tablets also taught me about mobile device security. Each device contained sensitive company data, so securing them was important. I checked authentication settings, ensured screen locks were properly configured, reviewed app permissions, and confirmed that no unauthorized apps were installed.

This experience deepened my understanding of mobile device management not only in a technical sense but in a practical, usercentered way.

VII. Building, Configuring, and Deploying Workstations

Building and configuring workstations was one of the most rewarding aspects of the internship. I helped assemble hardware, install operating systems, update drivers, configure user accounts, and set up workstations based on the preferences and responsibilities of each employee.

Building workstations from scratch taught me about hardware compatibility, BIOS settings, thermal management, and proper cable placement. Installing the operating system required attention to detail, as missing drivers or incorrect configuration could lead to performance issues later.

Once the hardware and OS were ready, I configured the workstation to meet company standards. This included installing required applications, configuring security settings, setting up email accounts, adjusting system preferences, connecting printers, and applying necessary updates.

These tasks strengthened my understanding of both the physical and digital aspects of computer setup. They also helped me appreciate the importance of consistency, documentation, and user-specific customization in IT environments.

VIII. Cybersecurity Practices, Vulnerabilities, and Improvements

One of the primary lessons from this internship was seeing how cybersecurity fits into a nontechnical industry. Many construction companies do not have dedicated cybersecurity departments, making it even more important that staff understand and practice basic security measures.

Throughout the internship, I observed several areas where security could be improved. For example, some employees used weak passwords or reused the same passwords across multiple devices. Others postponed software updates because they did not want to interrupt their work. There were also instances where sensitive data was stored locally instead of being uploaded to more secure storage systems.

I helped address these vulnerabilities by promoting stronger password usage, assisting with system updates, configuring automatic update settings, and helping employees understand why certain practices were necessary for protecting company data. These efforts taught me how cybersecurity must be approached with empathy, clear communication, and an understanding of workflow needs.

IX. Communication, Collaboration, and User Support

Working in IT requires strong communication skills, and this internship provided many opportunities to develop them. Many employees had limited technical backgrounds, which meant I needed to explain technical concepts in ways that were easy to understand.

When troubleshooting, I learned to ask clear questions to gather accurate information and avoid unnecessary steps. I also learned the importance of remaining calm and patient even when employees were frustrated or stressed about malfunctioning devices.

Collaboration with supervisors and coworkers also contributed to the flow of work. Whenever a more complex problem occurred, I discussed potential solutions with my supervisor and learned from their experience. This section of my internship helped me understand that cybersecurity work is not only technical, it is heavily people-focused.

X. Challenges, Troubleshooting, and ProblemSolving

I encountered many challenges during my internship, each of which strengthened my ability to think critically and solve problems under pressure. Some challenges were technical, such as diagnosing compatibility issues, resolving failed updates, or identifying faulty hardware. Others were workflow-related, such as balancing multiple tasks or communicating the importance of security practices to busy employees. Each challenge taught me the importance of methodical troubleshooting. Instead of jumping to conclusions, I learned to test possible causes step by step. This approach prevented unnecessary mistakes and helped resolve problems more efficiently. Overall, the challenges I faced helped me grow as both a technician and a future cybersecurity professional.

XI. Tools, Software, and Methods Used During the Internship

My internship exposed me to various tools and methods essential for IT support and cybersecurity. These included operating system utilities, mobile device management tools, cloud storage platforms, antivirus programs, and troubleshooting methods such as isolating variables and testing alternative configurations. Understanding how these tools worked together helped me gain a deeper appreciation for the technical ecosystem behind everyday business operations.

XII. Development of Technical and Professional Skills

Throughout the internship, I developed numerous technical skills such as device configuration, system updates, hardware installation, software troubleshooting, account management, and mobile device security. I also improved professional skills such as communication, organization, time management, documentation, and staying composed during unexpected issues. This combination of skills is essential for future cybersecurity roles and provides a strong foundation for continued growth.

XIII. Observations on Cybersecurity in NonTechnical Industries

One of the most valuable insights from this internship was seeing how cybersecurity functions in a nontechnical business. Many small and medium-sized companies rely heavily on technology but lack formal cybersecurity infrastructure. This makes the role of knowledgeable employees and strong security practices even more important. My experience showed me that cybersecurity is not limited to large corporations but applies everywhere.

XIV. Professional Growth and Workplace Adaptation

Working at Toano Contractors helped me grow professionally by improving my confidence, independence, and ability to handle realworld responsibilities. I learned how to adapt quickly, communicate with diverse groups of people, and manage both expected and unexpected tasks. These experiences prepared me for future professional environments.

XV. Influence on My Future Career Goals

Before my internship, I knew I wanted to work in cybersecurity, but I did not fully understand how broad the field was. This experience showed me the importance of combining cybersecurity knowledge with practical IT experience. It also inspired me to pursue roles that integrate technical security responsibilities with handson system support. The internship confirmed that I am on the right path.

XIII. Conclusion

My internship marked a defining period in my professional development, allowing me to grow not only as a cybersecurity student but as a developing practitioner who began to understand how security functions within the larger ecosystem of a business. Throughout my time with the company, I witnessed firsthand how cybersecurity decisions affect real people, real timelines, and real financial outcomes. This experience transformed my perspective on the field, shifting my understanding from purely technical concepts learned in the classroom to a recognition of how those concepts live, breathe, and evolve in fast-paced operational environments. I learned that cybersecurity is not an isolated discipline; it is deeply intertwined with communication, teamwork, training, and the daily realities of employees who rely on secure systems to perform their jobs.

Reflecting on the challenges and accomplishments I experienced, I can see how each task contributed to my development. Whether I was troubleshooting network issues, hardening security configurations, assisting employees who were unfamiliar with best practices, or learning to balance security with organizational usability, every moment pushed me to adapt, think critically, and solve problems with both precision and empathy. These experiences strengthened my confidence in my ability to manage responsibilities and make decisions rooted in security principles. They also deepened my appreciation for the importance of patience and clarity, especially when guiding users who depend on my knowledge to remain safe online.

As I look ahead to my future career, I recognize that this internship built the foundation I need to succeed in more advanced roles. The lessons I gained will shape how I approach risk, communication, and continuous learning. Ultimately, this internship reaffirmed my commitment to the cybersecurity field and showed me that my strengths, problem solving, attention to detail, adaptability, and the ability to communicate clearly are not only valuable but essential to

protecting organizations in an increasingly digital world. This experience did more than help me grow; it prepared me for the responsibilities and opportunities that lie ahead.