Matthew Surratt

Reflection Paper 1

Date: 06/16/2026

ODU Summer 2026

RiverTrail Technology

Professor Teresa Duvall/TA Jade Hines

Internship Reflections Paper

First 50 Hours

During my first 50 hours as a Cybersecurity Analyst Intern at RiverTrail Technology, I have gained valuable hands-on experience in cybersecurity risk management, compliance auditing, and vulnerability assessment. My primary responsibilities included assisting with a company-wide risk assessment and conducting a compliance audit related to the organization's cybersecurity insurance policy. These projects have provided me with practical exposure to how cybersecurity principles are applied in a business environment and have strengthened my understanding of risk management and regulatory compliance.

One of my first assignments was to assist with a compliance audit of RiverTrail Technology's cybersecurity insurance requirements. The purpose of this audit was to verify that the company was meeting the technical controls required by its cyber liability insurance policy. Through this process, I learned that cybersecurity insurance providers often require organizations to maintain specific security practices in order to qualify for coverage or successfully file a claim after a cyber incident.

A significant portion of the audit involved reviewing technical requirements and verifying that the organization was complying with them. For example, one requirement involved ensuring that data backups were being performed regularly and that backup restoration processes were tested periodically. This requirement highlighted the importance of not only creating backups but also validating that they can be successfully restored when needed. I learned that if an organization fails to maintain these required controls and experiences a data breach or ransomware attack, the insurance provider may deny coverage or reduce the payout.

Another valuable learning experience during my internship was participating in a Google Meet demonstration with Inscora, a company that provides cybersecurity assessment tools for Managed Service Providers. The platform allows MSPs to scan client networks and domains for vulnerabilities and assign risk scores based on the findings. While the tool performs functions similar to network scanning utilities such as Nmap, it consolidates multiple vulnerability assessments into a single platform and provides business-oriented risk reporting.

During the demonstration, I learned how MSPs can use vulnerability scanning and risk scoring tools to identify security weaknesses and help clients improve their overall security posture. Additionally, the risk scores generated by these assessments can assist organizations in qualifying for cybersecurity insurance by demonstrating that they are actively monitoring and addressing vulnerabilities.

In addition to the compliance audit, I began work on a risk assessment for RiverTrail Technology. Since the company operates as a Managed Service Provider (MSP), one of its primary concerns is the possibility of threat actors impersonating company personnel to gain access to clients or sensitive information. To evaluate this risk, I conducted passive reconnaissance and Open-Source Intelligence (OSINT) research on publicly available information related to the company owner and office manager.

Using search engines and AI-assisted OSINT techniques, I gathered publicly accessible information that could potentially be leveraged in a social engineering attack. My objective was not to collect private information, but rather to identify what information was already available online and determine how it could be used by an attacker. After compiling my findings, I assessed the associated risks and assigned risk levels based on the amount and sensitivity of information discovered. I also provided written explanations describing how each finding could contribute to potential social engineering or impersonation attacks.

One of the most interesting experiences during my first 50 hours at RiverTrail Technology was observing the investigation of a network security issue involving one of the company's clients. Although I was not directly involved in resolving the incident, it provided valuable insight into the importance of attention to detail in cybersecurity. The client reported receiving a "403 Forbidden" error whenever they attempted to access their online banking website. Initially, technicians investigated several common causes, including antivirus software, firewall rules, and potential blacklisting issues, but none of these appeared to be responsible for the problem. To determine the root cause, the bank was

contacted directly. The bank informed the technician that the company's public IP address had been blocked due to unusually high levels of network traffic. While it could not be conclusively determined whether the traffic was associated with a denial-of-service attack, botnet activity, or repeated login attempts, the excessive traffic was sufficient for the bank to block access from the client's network. With the cause identified, the next challenge was determining which device on the network was generating the traffic. As part of the investigation, employees were asked to disable Wi-Fi on their mobile phones, but network monitoring still detected four Android-based devices connected to the network. While searching the office for the source of these devices, technicians discovered four digital picture frames, one located in each office. Three of the devices were from well-known manufacturers, while one was an unbranded device. After the unbranded digital picture frame was unplugged, the abnormal network traffic immediately stopped. This incident served as a real-world example of the risks associated with Internet of Things (IoT) devices. Throughout my cybersecurity education at Old Dominion University, I had learned about the potential dangers of poorly secured IoT devices, but witnessing an actual incident reinforced the importance of monitoring all devices connected to a network. This experience demonstrated how even seemingly harmless devices can create significant security concerns and highlighted the need for cybersecurity professionals to carefully investigate every possible source of network activity.

Overall, my first 50 hours at RiverTrail Technology provided meaningful exposure to several core cybersecurity disciplines, including compliance auditing, risk assessment, OSINT investigations, and vulnerability management. These experiences have allowed me

to apply concepts learned in the classroom to real-world business scenarios while developing a deeper understanding of how cybersecurity supports organizational risk management.