

Internship Report

Cybersecurity Risk Management and Framework Adaptation for Small Businesses

Submitted To:

Macquarie University
Department of Computing

Submitted By:

Tayyab Hameed
Student ID: 47644850
Session: 1, 2025

Organization Name:

Centropy Services & Solutions

Submission Date:

April 26, 2025



MACQUARIE
University
SYDNEY · AUSTRALIA

Acknowledgement

I would like to express my sincere gratitude to Mr. Amin Behasti for his unwavering support and guidance throughout my internship journey. From assisting with the availability letter to facilitating my participation in the PACE partner session, his efforts were invaluable in helping me get started with confidence.

I am thankful to the Professional and Community Engagement (PACE) team at Macquarie University for organizing the industry engagement session and enabling access to this internship opportunity. Their commitment to connecting students with industry professionals was instrumental in enriching my learning experience.

My heartfelt appreciation goes to Ms. Vandana Khanna, Delivery Partner at Centropy Services & Solutions, for accepting me as an intern and providing continuous mentorship throughout the internship. Her expertise in cybersecurity risk management and strategic oversight helped me understand the implementation of practical security frameworks in real-world scenarios.

I also extend my thanks to Mr. Varun Batra, Managing Director at Centropy, for his engagement, encouragement, and guidance. His deep experience in cybersecurity, governance, and digital transformation helped me better understand how cybersecurity aligns with broader organizational goals and compliance obligations.

Finally, I thank the entire Centropy team for welcoming me into their professional environment and the Macquarie University Department of Computing for integrating this valuable industry-based learning into the curriculum.

Executive Summary

This report presents a comprehensive account of an internship conducted at a cybersecurity consultancy firm focused on Governance, Risk, and Compliance (GRC). The primary objective of the internship was to support the development of a simplified cybersecurity framework tailored to small and medium-sized enterprises, using the NIST Cybersecurity Framework (CSF) 2.0 as the baseline.

The internship was divided into two distinct phases. In the first phase, the intern conducted an Open-Source Intelligence (OSINT) assessment of a healthcare organization (*Organization A*), identifying potential security exposures in its publicly accessible digital infrastructure. The findings were then mapped to relevant NIST CSF subcategories, revealing gaps across the Protect, Identify, and Respond functions. A detailed set of remediation recommendations was developed to address these weaknesses.

In the second phase, a similar OSINT assessment was performed on an educational institution (*Organization B*). The investigation involved domain and infrastructure mapping, vulnerability enumeration, and technology stack analysis. A total of 22 vulnerabilities were identified and aligned with specific NIST CSF controls. Actionable recommendations were drafted to help the organization reduce its public attack surface and improve its risk posture.

Throughout the internship, the intern applied passive reconnaissance methods, documented vulnerabilities, analysed security control gaps, and contributed to building a practical cybersecurity roadmap aligned with industry standards. This report includes reflective journal entries, anonymized work samples, and a critical analysis of the technical and strategic lessons learned during the internship.

Table of Contents

ACKNOWLEDGEMENT	2
EXECUTIVE SUMMARY	2
OVERVIEW OF THE ORGANIZATION	6
a. Brief History.....	6
b. Introduction of the Organization.....	6
c. Policy of the Organization.....	6
d. Competitors of the Organization	7
ORGANIZATIONAL STRUCTURE	7
a. Organizational Hierarchy Chart.....	7
b. Number of Employees	7
c. Main Offices	8
d. Introduction of All the Departments.....	8
e. Comments on the Organizational Structure.....	8
INTERNSHIP SCHEDULE AND DEPARTMENTAL ENGAGEMENT.....	8
a. Introduction of the Office	8
b. Starting and Ending Dates	8
c. Internship Type	9
d. Departments and Duration of Training	9
TRAINING PROGRAM.....	9
Introduction	9
Phase 1 – Weeks 1–4.....	9
Phase 2 – Weeks 5–8.....	10
Phase 3 – Weeks 9–12	10
Tools and Skills Gained	11
Conclusion	12
JOURNAL ENTRIES.....	12
WEEK 1 (26 FEB – 3 MAR 2025) – REFLECTIVE JOURNAL ENTRY.....	12
WEEK 2 (4 MARCH – 10 MARCH 2025) – REFLECTIVE JOURNAL ENTRY.....	13
WEEK 3 (11 MARCH – 17 MARCH 2025) – REFLECTIVE JOURNAL ENTRY.....	14
WEEK 4 (18 MARCH – 24 MARCH 2025) – REFLECTIVE JOURNAL ENTRY.....	14
WEEK 5 (25 MARCH – 31 MARCH 2025) – REFLECTIVE JOURNAL ENTRY.....	15
WEEK 6 (1 APRIL – 7 APRIL 2025) – REFLECTIVE JOURNAL ENTRY.....	16
WEEK 7 (8 APRIL – 14 APRIL 2025) – REFLECTIVE JOURNAL ENTRY.....	16
WEEK 8 (15 APRIL – 21 APRIL 2025) – REFLECTIVE JOURNAL ENTRY.....	17
WEEK 9 – REFLECTIVE JOURNAL ENTRY	18
WEEK 10 – REFLECTIVE JOURNAL ENTRY	18
WEEK 11 – REFLECTIVE JOURNAL ENTRY	19
WEEK 12 – REFLECTIVE JOURNAL ENTRY	19
WORK SAMPLES.....	19
WORK SAMPLE 1: OSINT-BASED SECURITY ASSESSMENT FOR A REGIONAL HEALTHCARE PROVIDER	19
WORK SAMPLE 2: OSINT-BASED SECURITY ASSESSMENT FOR A PUBLIC EDUCATIONAL INSTITUTION	23
WORK SAMPLE 3: PHISHING INCIDENT IDENTIFICATION AND ANALYSIS REPORT.....	26
CRITICAL ANALYSIS	30
SWOT ANALYSIS	32
STRENGTHS	32
WEAKNESSES.....	33
OPPORTUNITIES	33

THREATS	34
CONCLUSION	35
RECOMMENDATION	35
REFERENCES:	36

Overview of the organization

a. Brief History

The host organization for this internship is **Centropy**, a Sydney-headquartered Australian-owned boutique professional services firm. Established with the aim of supporting organizations through complex technology and risk transformations, Centropy has grown by combining deep domain knowledge with multidisciplinary expertise. The firm is composed of seasoned consultants and advisors with experience across industries such as finance, healthcare, education, and government, and has earned a reputation for delivering practical, results-driven solutions.

The name “Centropy” symbolizes the coming together of structure, method, and strategy. True to its name, the firm emphasizes cohesion in how technology, governance, and process maturity are aligned to enhance business outcomes.

b. Introduction of the Organization

Centropy specializes in **Assurance, Advisory, and Software Managed Services**, with a core focus on **Governance, Risk, and Compliance (GRC)** and **Cybersecurity**. The organization helps its clients **reduce business risks, strengthen internal controls, and streamline business operations** in line with regulatory and industry standards.

Centropy delivers services across the domains of:

- IT Risk and Cybersecurity Strategy
- Security Governance Frameworks
- Compliance Mapping (e.g., NIST CSF, ISO 27001, Essential Eight)
- Vulnerability Assessments and OSINT Investigations
- Risk Control Design and Implementation
- Policy and SOP Development

Clients range from mid-sized businesses to public sector institutions, many of which require cost-effective, yet robust cybersecurity frameworks tailored to their needs. A typical engagement includes security posture assessments, the identification of control gaps, and advisory on how to implement prioritized mitigations using global standards.

Centropy’s mission is to **simplify complex cybersecurity problems**, enhance operational maturity, and help organizations improve their **ICT security posture**. It achieves this through a pragmatic approach, avoiding theoretical overengineering in favor of actionable, scalable recommendations.

c. Policy of the Organization

Centropy maintains a strong **code of conduct and ethics**, emphasizing professionalism, confidentiality, and respect for client trust. Internally, the company operates using an ISO 9000-based **Quality Management System (QMS)**, which guides delivery practices, documentation standards, and client satisfaction metrics.

Quality is a foundational value, and all team members are trained in Centropy's structured methodology, which includes templates, precedents, and best practice notes. Regular internal audits and feedback loops ensure continual improvement.

Centropy's work is also governed by a strong emphasis on **compliance**, aligning projects with national and international standards. For interns, this meant adhering strictly to non-disclosure obligations, anonymization of sensitive data, and learning how formal security practices are embedded in organizational workflows.

d. Competitors of the Organization

Centropy operates in a competitive industry with several local and international firms offering similar GRC and cybersecurity services. Notable competitors include mid-tier consulting firms such as Protiviti, BDO Cybersecurity, and Shearwater Solutions, along with larger entities like PwC and Deloitte that offer overlapping cybersecurity risk advisory services.

Centropy differentiates itself by focusing on small to mid-sized clients, offering cost-effective, pragmatic, and personalized engagement models. Unlike larger firms, Centropy offers greater flexibility and closer ongoing advisory relationships, making it a preferred partner for organizations that require hands-on support without enterprise-level costs.

Organizational Structure

a. Organizational Hierarchy Chart

Centropy Services & Solutions operates with a streamlined organizational structure designed to facilitate efficient decision-making and client service delivery. The hierarchy is as follows:

- **Managing Director:** Mr. Varun Batra
- **Delivery Partner:** Ms. Vandana Khanna
- **Consultants and Analysts:** A team of cybersecurity and GRC professionals
- **Interns:** Students and trainees engaged in practical learning

This structure promotes direct communication and collaboration across all levels, ensuring that strategic decisions align with operational execution.

b. Number of Employees

Centropy maintains a core team of approximately 9 employees, as reported by Datanyze . This lean team is supplemented by a network of partner organizations and associates, allowing the company to scale its services according to client needs while maintaining personalized attention.

c. Main Offices

The company's headquarters is located in Wahroonga, New South Wales, Australia. This central location enables Centropy to effectively serve clients across the Sydney metropolitan area and beyond.

d. Introduction of All the Departments

Centropy's operations are divided into several key departments:

- **Advisory Services:** Provides strategic guidance on IT governance, risk management, and compliance frameworks.
- **Assurance Services:** Conducts audits and assessments to ensure clients meet regulatory and industry standards.
- **Managed Services:** Offers ongoing support for cybersecurity infrastructure, including monitoring and incident response.
- **Training and Development:** Delivers educational programs to enhance client and internal team capabilities in cybersecurity practices.

Each department works collaboratively to deliver comprehensive solutions tailored to client requirements.

e. Comments on the Organizational Structure

Centropy's organizational structure is characterized by its agility and collaborative approach. The flat hierarchy facilitates quick decision-making and fosters a culture of open communication. The integration of partner organizations and associates allows for flexibility in scaling services and accessing specialized expertise. This structure supports Centropy's mission to provide pragmatic and implementable advice in the areas of IT, GRC, and cybersecurity.

Internship Schedule and Departmental Engagement

a. Introduction of the Office

The internship was conducted at the Sydney-based head office of a boutique cybersecurity consultancy firm specializing in Governance, Risk, and Compliance (GRC). The organization operates in a hybrid capacity, with a core team based in New South Wales and a distributed delivery model that engages clients remotely across various industries. The team works in close coordination via virtual stand-ups and collaboration platforms, providing interns with direct access to senior consultants and delivery partners throughout the project lifecycle.

b. Starting and Ending Dates

The internship commenced on **February 28, 2025**, and is scheduled to conclude on **May 28, 2025**, covering a duration of **13 weeks** as per Macquarie University's academic requirement for industry-based learning under the PACE program.

c. Internship Type

This was a **full-time internship**, allowing for immersive participation in organizational workflows, project planning sessions, client risk assessments, and security documentation efforts.

d. Departments and Duration of Training

Over the course of the internship, I was actively involved in the **Cybersecurity Advisory** and **Assurance** departments. The training was structured into two distinct 4-week blocks:

- **Weeks 1–4: Cybersecurity Risk Advisory**
I participated in client-facing risk assessments, OSINT investigations, and NIST CSF control mapping for a healthcare sector organization (referred to here as *Organization A*).
- **Weeks 5–8: Vulnerability Assessment & Security Governance**
I performed digital footprint analysis, vulnerability identification, and strategic control recommendations for a public educational institution (*Organization B*), aligned with NIST CSF functions.

Additionally, time was dedicated to refining outputs, preparing formal reports, and contributing to reusable security templates and frameworks designed to support small business clients with limited cybersecurity resources.

Training Program

Introduction

This section presents an in-depth account of the internship experience, including the operations, tasks, tools, and learning outcomes achieved through two core project phases. Each phase reflects real-world cybersecurity practices targeting the risk landscapes of two distinct sectors—healthcare and education—offering valuable insights into how digital security frameworks are applied in organizational settings.

Phase 1 – Weeks 1–4

Client: A regional healthcare provider
Department: Cybersecurity Advisory

In the first phase of the internship, I worked closely with the Cybersecurity Advisory team to conduct a comprehensive OSINT-based security assessment for a regional healthcare provider. This engagement focused on identifying externally visible digital assets and evaluating their exposure to potential threats. My tasks involved passive reconnaissance, including subdomain enumeration through tools like crt.sh and DNSDumpster, fingerprinting infrastructure using Shodan and BuiltWith, and documenting misconfigured services.

During this process, I identified 22 security weaknesses, including publicly exposed WordPress login panels, outdated CMS installations, missing security headers, and absence

of two-factor authentication. I further leveraged curl, browser dev tools, and the Wayback Machine to understand historical changes in security configurations. Each vulnerability was mapped to corresponding NIST CSF subcategories such as PR.AC-1 (Access Control), PR.DS-2 (Data-in-Transit Protection), and ID.AM-1 (Asset Management). I also developed a comprehensive remediation plan prioritizing low-cost, high-impact controls suitable for a resource-limited healthcare environment.

This phase honed my ability to translate technical findings into actionable guidance. I learned to write executive-level summaries, develop visual control-mapping matrices, and align findings with compliance frameworks. All findings were compiled into a formal client-ready report.

Phase 2 – Weeks 5–8

Client: A public educational institution

Department: Security Governance and Assessment

In the second half of the internship, I collaborated with the Assurance and Governance team to assess the digital security posture of a public educational institution. I began with reconnaissance using tools such as Amass, crt.sh, and DNSDumpster to identify active subdomains, followed by service mapping through reverse IP analysis and certificate transparency logs. My OSINT investigation revealed critical vulnerabilities including an exposed Plesk hosting panel, metadata leakage via unprotected AWS S3 buckets, predictable document paths, and multiple legacy login pages.

Using exiftool and mat2, I extracted metadata from academic documents, revealing usernames and document generation details. I also used dirsearch to identify hidden directories, some of which returned 403 responses—signaling the existence of potentially sensitive assets. Each issue was analyzed against exploitability, impact, and risk category and mapped to relevant NIST CSF subcategories like PR.DS-6 (Data Integrity), ID.AM-3 (Inventory of External Systems), and RS.AN-1 (Security Analysis).

I documented 9 vulnerabilities and prepared a technical recommendation plan focusing on access restrictions, policy enforcement, and metadata sanitation. This included proposed control actions such as implementing CAPTCHA, disabling native logins, restricting Plesk access to whitelisted IPs, and applying Subresource Integrity (SRI) on JavaScript libraries.

One notable challenge in this phase was assessing risk under a shared hosting environment. This introduced complexities in identifying true asset ownership, which I mitigated using WHOIS and CDN fingerprinting. The work was presented in a structured risk report with supporting visuals and executive insights.

Phase 3 – Weeks 9–12

Client: Continued engagements with masked organizations and internal deliverables

Department: Cybersecurity Governance and Framework Development

In the final phase of the internship, my work transitioned from technical assessments to solution design, compliance alignment, and internal documentation development. I collaborated with senior consultants to convert previously discovered vulnerabilities into

practical, actionable recommendations aligned with the NIST Cybersecurity Framework (CSF) and other standards.

In Week 9, I focused on developing a comprehensive set of remediation strategies for vulnerabilities identified in earlier assessments. These solutions were categorized by technical control type, business feasibility, and implementation complexity. Recommendations included both preventive and detective measures and were designed for resource-constrained environments. Each control action was aligned with corresponding NIST CSF subcategories.

In Week 10, I designed a reusable cybersecurity assessment questionnaire aimed at evaluating the baseline security posture of organizations. The document was structured into core thematic sections—Identity & Access Management, Network Security, Incident Response, and Data Protection. It was piloted using a masked organization, and the output provided insights into the organization's maturity across governance, technical safeguards, and user awareness. The format was kept simple and non-technical to encourage adoption by small and mid-sized businesses.

Week 11 involved a deep dive into Digital Operational Resilience Act (DORA) compliance mapping for a financial-sector client. I reviewed DORA's requirements and translated them into a clear and concise checklist that included evidence expectations and assessment guidance. The checklist covered ICT risk management, business continuity, third-party oversight, and incident response capabilities. The mapping exercise helped identify compliance gaps and potential improvements and provided the organization with a practical implementation path.

Finally, in Week 12, I consolidated the outcomes of all major tasks completed during the internship. I participated in a formal feedback session with my supervisor, during which I presented a summary of deliverables including the NIST CSF roadmap, security templates, OSINT findings, and compliance checklists. I incorporated final feedback into the documents and reflected on key personal and technical lessons. This phase emphasized the importance of stakeholder communication, report readability, and adaptability when translating security assessments into business-aligned actions.

Tools and Skills Gained

Tools Used:

- **OSINT & Enumeration:** Shodan, crt.sh, DNSDumpster, SecurityTrails, Amass, Wayback Machine
- **Scanning & Analysis:** Nmap, dirsearch, BuiltWith, browser dev tools
- **Metadata & Exposure:** exiftool, mat2, curl
- **Documentation & Mapping:** CVE databases, NIST CSF 2.0 documentation, DORA compliance framework
- **Template & Report Design:** Google Docs/Sheets, Microsoft Word, internal Centropy templates
- **Assessment Tools:** Self-developed cybersecurity questionnaire, checklist-based gap analysis formats

Skills Developed:

- Passive reconnaissance and subdomain enumeration
- Identification and analysis of exposed services and misconfigurations
- Metadata extraction and interpretation
- Mapping vulnerabilities to NIST CSF control functions and subcategories
- Writing structured cybersecurity assessment reports
- Translating technical data into executive-level recommendations
- Strengthening communication, presentation, and documentation skills
- Delivering simplified roadmaps and policy recommendations
- Working independently and iteratively within a hybrid consulting model

Conclusion

The internship offered a transformative learning experience by blending academic knowledge with real-world cybersecurity practice. It provided hands-on exposure to how organizations across sectors manage digital risk, structure their IT governance, and implement security controls. The process of discovering, documenting, and analyzing vulnerabilities deepened my understanding of adversarial thinking, compliance requirements, and security architecture. Most importantly, I learned how to communicate complex technical risks to both technical and non-technical stakeholders, which is a critical skill in the cybersecurity domain.

In the final phase of the internship, I expanded my role from assessment to solution development, compliance mapping, and framework design. Tasks such as developing a cybersecurity questionnaire, mapping organizational gaps to the DORA regulatory framework, and finalizing a tailored NIST CSF implementation roadmap helped me grow into a more well-rounded security consultant. I also learned the value of structure and simplicity in delivering recommendations that small businesses can realistically adopt.

The hybrid nature of the internship allowed me to take ownership of my work while regularly interacting with experienced professionals. Whether documenting phishing threats, designing checklists, or mapping vulnerabilities to frameworks, every task contributed to my confidence and capability in applying cybersecurity principles to real-world environments. This internship has helped shape my mindset toward continuous learning, regulatory awareness, and practical risk mitigation — qualities that I will carry forward into my professional journey.

Journal Entries

Week 1 (26 Feb – 3 Mar 2025) – Reflective Journal Entry

Describe:

The first week of my internship mainly involved settling into the organization and understanding the project I would be working on. I attended an onboarding session where I was introduced to Centropy's main focus areas, especially how they work with Governance, Risk, and Compliance (GRC). I was assigned to work on a cybersecurity risk assessment for a healthcare client. My first task was to gather information about the client's environment through open-source methods. I spent time using tools like Shodan, DNSDumpster, crt.sh, and basic WHOIS lookups to start building an external profile of the client's infrastructure. I also

began to familiarize myself with the NIST Cybersecurity Framework (CSF) because it would be central to my work moving forward.

Interpret:

This week gave me my first real taste of how cybersecurity works outside the classroom. It's one thing to study frameworks and tools in theory, but actually applying them to a live client's environment felt very different. I realized that information gathering isn't just running a few tools, it's about thinking carefully, connecting different pieces, and building a full picture from fragments. It made me understand the value of patience and being methodical. It also made me realize that even small bits of public information can reveal a lot about an organization's security posture if someone knows how to look for it.

Evaluate:

Overall, I think I adjusted well to the new environment. I was a bit slow at first because I wanted to be very careful with my OSINT methods, but I gained confidence once I saw how much useful information I could pull with non-intrusive techniques. One challenge was that some of the data was outdated or confusing (especially DNS records), but I managed to cross-reference sources to make sure my findings were still valid. I felt like I started understanding what it means to think like an attacker, and that was a shift from just "following steps" in university labs.

Plan:

In the next few weeks, I want to get faster and more accurate in my information gathering. I also plan to start thinking more about risk, not just finding vulnerabilities, but understanding what they could actually mean for a real business. I'm aiming to improve the way I document and organize findings too, so they're easier to use when I have to map them to NIST CSF controls later on.

Week 2 (4 March – 10 March 2025) – Reflective Journal Entry

Describe:

This week, I worked on taking the information I collected during the OSINT phase and started mapping it into the NIST Cybersecurity Framework (CSF) structure. I reviewed each identified vulnerability or exposure and tried to understand where it would fit within the five functions (Identify, Protect, Detect, Respond, Recover) and the subcategories under them. I had some sessions with my supervisor where we discussed real-world examples of how organizations prioritize cybersecurity risks and how frameworks like NIST CSF help guide risk management. I spent most of the week writing a draft of the initial mapping document, which included matching security gaps to specific control areas.

Interpret:

Working with the NIST CSF practically made me realize how flexible yet challenging the framework is. In university, we study frameworks like something you can just "apply," but in reality, it's more about interpreting each finding within the business context. I noticed that many vulnerabilities could actually fit under multiple subcategories, depending on how you looked at them. This forced me to think not just technically, but strategically. I also saw how different industries, like healthcare in this case, have their own nuances when it comes to applying controls. Patient data protection has very specific needs compared to general IT environments.

Evaluate:

This week really challenged my thinking, but in a good way. I wasn't just analyzing a vulnerability like "this server is exposed," but asking "what does this exposure mean for this type of organization?" Initially, I found it confusing when the same issue seemed to touch multiple CSF areas. But after reviewing examples and talking with my mentor, I started feeling more confident. One thing I need to improve is being quicker in deciding which control is the

"best fit" without second-guessing myself too much. I realized cybersecurity isn't always black and white, context matters a lot.

Plan:

Next week, I plan to refine my control mapping by creating a standard process or checklist I can reuse for other organizations. I also want to become more comfortable explaining my mapping logic clearly in reports, especially since clients might not always be technical. My goal is to make my reporting more organized and ensure that my recommendations are tied directly back to specific CSF subcategories, so that the client knows exactly what to improve and why.

Week 3 (11 March – 17 March 2025) – Reflective Journal Entry

Describe:

In Week 3, I shifted my focus from framework mapping to conducting a deeper Open-Source Intelligence (OSINT) investigation for the healthcare provider. This time, I explored their external digital footprint more extensively by looking into subdomains, certificate transparency logs, email systems, cloud storage exposure, and public-facing login portals. I used tools like crt.sh, Amass, SecurityTrails, and the Wayback Machine to find historical exposure data. I also practiced passive scanning through Nmap to banner grab certain services and validate whether outdated technologies were in use. I began building a network diagram showing the discovered infrastructure and potential risk points.

Interpret:

This week made me realize how much information is out there publicly, and how even organizations that think they are secure can have exposures without realizing it. Finding login portals, subdomains linked to third parties, and metadata leaks without even touching their systems showed me how dangerous simple misconfigurations can be. It also reinforced how attackers operate: slowly gathering bits and pieces over time before launching more aggressive attacks. I also noticed how technical findings start to interconnect. For example, an exposed WordPress login panel, paired with outdated plugins, creates a serious risk chain.

Evaluate:

I think I did a good job in systematically expanding my reconnaissance and cross-validating my findings. One thing I struggled with at first was managing the huge amount of data, it was easy to get overwhelmed. I realized that documenting everything clearly while I worked (screenshots, short notes) saved me a lot of time later when building the reports. My supervisor liked that I presented findings in a structured way instead of dumping raw data, which made me realize how important communication is even when doing technical work. However, I still feel I can improve on filtering noise versus true risks more quickly.

Plan:

Going forward, I want to refine my OSINT methodology by creating a checklist of key areas to investigate, so I don't miss important exposures but also don't waste time chasing irrelevant data. I also plan to start tying findings directly to potential threat scenarios (e.g., credential stuffing, phishing attacks), so that my reports are not just technical but also risk-driven. Understanding how findings translate into real-world attacks will make my work more valuable and professional.

Week 4 (18 March – 24 March 2025) – Reflective Journal Entry

Describe:

In Week 4, I finalized the OSINT findings for the healthcare client and started preparing a detailed documentation report. I focused on creating structured sections: asset discovery, technology stack analysis, vulnerabilities identified, and risk prioritization. I documented 22 vulnerabilities in total, categorized by severity. Each finding included a brief description, the

method of discovery, and a potential risk impact. I also worked on creating a remediation recommendation table that suggested practical and affordable solutions, considering that the client was a small healthcare provider. I presented a draft report to my supervisor for initial feedback.

Interpret:

This week taught me how different the real-world reporting process is compared to university assignments. It is not just about listing vulnerabilities. It is about presenting the information in a way that makes sense to someone who may not be technical. I realized that too much technical detail can confuse or overwhelm a client. Instead, focusing on explaining the "risk" and "impact" helps the client understand why a vulnerability matters. This made me think differently about my role. I am not just finding issues; I am helping clients understand their security weaknesses in a way they can act on.

Evaluate:

I felt I was getting much better at writing professionally and logically. One thing I noticed was that I sometimes still used too much technical jargon in my first drafts. My supervisor's feedback helped me simplify my language without losing the technical meaning. I also learned the value of presenting solutions alongside problems. When I recommended fixes like implementing CAPTCHA, restricting access to admin panels, or enforcing SSL, it made the report more actionable. Overall, I was happy with how much I improved in delivering work that could be used in a real business setting.

Plan:

Next, I want to keep practicing writing in a more client-friendly tone without losing technical accuracy. I also plan to improve my visual presentation of findings. For example, using small diagrams or tables to summarize exposures could make future reports even easier to read. Going forward, I will focus not only on technical depth but also on how clearly and persuasively I can communicate cybersecurity risks and solutions to different audiences.

Week 5 (25 March – 31 March 2025) – Reflective Journal Entry

Describe:

In Week 5, I started working on a new organization, a public educational institution. I shifted my focus from the healthcare sector to the education sector, which presented a slightly different set of cybersecurity challenges. My main task this week was to begin an OSINT investigation for the institution. I started by using tools like crt.sh, Amass, and DNSDumpster to enumerate their subdomains and infrastructure. I also gathered information on their login portals, cloud storage setups, and service providers. Unlike the healthcare client, this institution had a more public-facing digital footprint, which made the investigation more detailed and layered.

Interpret:

Working on a different sector helped me understand that every organization has a unique risk surface depending on how it operates. The educational institution had multiple public-facing services like student portals, printing services, and learning management systems, which meant more potential entry points for attackers. I realized that publicly available information, if not managed properly, can expose organizations to a wide range of threats. I also noticed that despite having some modern setups, there were clear signs of legacy systems still in use. This made me appreciate how real-world organizations often carry old infrastructure alongside new systems, which increases complexity and risk.

Evaluate:

This week felt more challenging than previous ones because there was a lot more data to process. I had to be very methodical in organizing the findings. One mistake I initially made was assuming that all detected subdomains were active without verifying them. After discussing it with my supervisor, I learned to perform proper checks to confirm if services were

live. I also noticed that the educational institution's public services were a bit more difficult to analyze due to heavy use of Cloudflare, which masked a lot of direct infrastructure information. Still, by cross-verifying data from multiple tools, I was able to map out a clear structure.

Plan:

Next week, I plan to dive deeper into vulnerability discovery by not just mapping services, but assessing their security configurations. I want to start identifying outdated software versions, open admin panels, and weak configurations where possible through passive techniques. I will also work on refining my reporting structure to make sure I capture each finding clearly and connect it directly to risk scenarios. My aim is to become faster at moving from raw data collection to meaningful security analysis.

Week 6 (1 April – 7 April 2025) – Reflective Journal Entry

Describe:

In Week 6, I continued the OSINT investigation for the educational institution, moving beyond asset discovery into deeper analysis. My focus was on identifying vulnerabilities in the external infrastructure. I used dirsearch to perform safe directory and file enumeration on public web servers. I also used exiftool and mat2 to analyze public documents for hidden metadata, such as usernames, software versions, and document creation timestamps. Additionally, I mapped cloud storage exposures by inspecting S3 bucket configurations through URL testing. I started compiling all these findings into a structured vulnerability list with descriptions and initial risk ratings.

During this week, an unexpected event also occurred. I received a phishing email impersonating a senior executive from Centropy. Recognizing signs like the use of a public domain email and urgent, suspicious language, I flagged the email immediately and reported it to my executive. I was later asked to conduct a formal analysis of the phishing attempt and prepare a detailed report on its tactics, source, and objectives.

Interpret:

This week helped me see how passive information gathering can uncover serious risks without touching or scanning a network aggressively. I realized that metadata embedded in documents can reveal a lot about an organization's internal systems and staff. Similarly, analyzing a real phishing attempt showed me that social engineering threats are equally important to watch for. It reinforced the idea that cybersecurity is not only about technical vulnerabilities but also about human factors like awareness, critical thinking, and communication.

Evaluate:

I think my technical work was solid this week, especially in using new tools like exiftool and mat2 that I had only studied before. I felt more confident in investigating non-obvious risks like metadata exposure and cloud misconfigurations. Handling the phishing incident gave me extra confidence that I can react professionally under pressure. One thing I struggled with was initially organizing the large number of small findings into a coherent report, but I adapted quickly with guidance from my supervisor.

Plan:

Going forward, I will work on creating a better reporting format where I group vulnerabilities clearly based on their risk impact. I also plan to learn more about cloud service security, especially AWS S3 configurations, and deepen my knowledge of social engineering threats. Building habits around fast incident escalation, accurate analysis, and organized reporting will help me become a more complete cybersecurity professional.

Week 7 (8 April – 14 April 2025) – Reflective Journal Entry

Describe:

In Week 7, my main focus was vulnerability enumeration for the educational institution based

on the infrastructure I mapped earlier. I started identifying outdated technologies, exposed login portals, metadata issues, and weak cloud configurations. I cross-checked public CVE databases to understand what known vulnerabilities were associated with the versions of technologies I found. I also explored login portals like WordPress admin pages, Plesk panels, and Office 365 SSO integrations, trying to assess their exposure levels without any intrusive testing. I documented each vulnerability with details like affected system, risk description, and possible exploitation paths.

Interpret:

This week taught me how important passive vulnerability analysis can be when done properly. Even without touching internal systems, just using public information and smart analysis techniques, it was possible to build a fairly complete risk profile. I also realized that it is easy to miss important small details if you rush through OSINT work. For example, a simple missing CAPTCHA on a login page can lead to brute force attacks, but it is easy to overlook when focusing only on big exposures. Another important insight was seeing how small misconfigurations like predictable S3 bucket paths or outdated JavaScript libraries could combine to create real attack chains.

Evaluate:

I felt proud of the quality of my vulnerability enumeration this week. I took more time verifying every finding, cross-checking it against risk databases and industry best practices. One area I know I can improve is speeding up my initial screening process. Sometimes I spent too long double-checking basic exposures when a simple rule-based triage would have been more efficient. I also realized that it is important to tailor the depth of investigation based on the client type. For example, some risks are much more critical for an educational institution handling student data than they would be for another type of organization.

Plan:

In the coming week, I plan to finalize the vulnerability list and start mapping each finding back to the NIST CSF framework, just like I did for the healthcare client. I also want to improve how I summarize vulnerabilities for reports, making it clear what the risk is, why it matters, and what simple actions could fix it. Learning to think like both an attacker and a defender will be my ongoing goal as I move forward in cybersecurity consulting.

Week 8 (15 April – 21 April 2025) – Reflective Journal Entry

Describe:

This week coincided with the Easter holidays, including Good Friday on 18 April and Easter Monday on 21 April. However, because the internship structure at Centropy was hybrid and flexible, it did not affect my work pace much. I continued working independently from home, focusing on finalizing the OSINT report for the educational institution. I spent time cleaning up the vulnerability documentation, making sure all findings were mapped properly to the NIST CSF framework. I also drafted a full set of recommendations tailored for the client, ensuring they were practical and suitable for an educational environment.

Interpret:

This week helped me understand the importance of self-discipline when working remotely. Even though it was technically a public holiday period, I preferred to keep working to maintain my momentum and complete my reporting tasks on time. I realized that in cybersecurity consulting, deadlines and deliverables often matter more than strictly sticking to office schedules. This experience also reinforced the habit of reviewing my own work critically before submission. Going back through earlier findings, I caught a few small details that I missed initially, which showed me how valuable second reviews are.

Evaluate:

I think I managed my time well this week, despite the holidays. Working independently without

direct supervision made me more confident in trusting my own judgment. One thing I could have improved was setting a clearer checklist for report completion earlier in the week. I spent a bit more time than necessary reformatting sections when I could have planned it better from the start. But overall, I was satisfied that I finished the technical findings, NIST mapping, and initial recommendation sections without delays, even in a shorter working week.

Plan:

Going forward, I want to develop a stronger habit of building report templates early in a project. This will help me organize findings better and save time during final documentation phases. I also want to get faster at critically reviewing technical writing, making sure that my reports are not just correct but also clean, professional, and easy to understand for clients. Being able to deliver good quality work even under flexible conditions is something I will definitely need in my future cybersecurity career.

Week 9 – Reflective Journal Entry

Describe:

This week, I focused on developing tailored mitigation strategies for the vulnerabilities previously identified during OSINT investigations. I reviewed each issue and created specific recommendations categorized by risk severity and feasibility. The goal was to ensure that solutions were practical for small businesses and aligned with NIST CSF subcategories.

Interpret:

This task pushed me to move beyond identification and into solution development. It made me think from the client's perspective, what steps would actually be realistic to implement given limited resources? It helped me appreciate that cybersecurity recommendations must strike a balance between thoroughness and operational simplicity.

Evaluate:

I was able to translate technical weaknesses into clear action items. One challenge was writing guidance in a way that non-technical readers could understand without oversimplifying. I improved my ability to communicate risk and controls in business-friendly language.

Plan:

Next week, I plan to package these recommendations into a structured implementation roadmap and begin drafting a new assessment tool to evaluate organizational posture.

Week 10 – Reflective Journal Entry

Describe:

I developed a cybersecurity questionnaire to assess the baseline security posture of small to mid-sized organizations. The document was structured around identity management, access controls, incident response, and data protection. I tested the format with a masked organization to ensure usability and coverage.

Interpret:

Creating this tool helped me internalize what baseline controls really look like and how to phrase questions to uncover gaps without using technical jargon. It also helped me understand how frameworks can be operationalized into client-ready tools.

Evaluate:

The initial version was well received, though I revised several questions to make them less technical and more scenario based. The challenge was ensuring completeness without making the questionnaire overwhelming.

Plan:

I plan to finalize the checklist for internal use and begin working on a regulatory compliance checklist based on the DORA framework in Week 11.

Week 11– Reflective Journal Entry

Describe:

This week, I worked on mapping an organization's controls against the Digital Operational Resilience Act (DORA). I developed a checklist with clear evidence requirements for ICT risk management, incident response, and governance, tailored for a financial-sector client.

Interpret:

This was my first exposure to DORA, and it expanded my view of how legal and regulatory requirements shape cybersecurity implementation. I learned to translate broad legal statements into measurable, practical controls.

Evaluate:

I found it rewarding to connect compliance requirements with actual technical and policy measures. One challenge was interpreting vague language in DORA and breaking it down into actionable items. I also practiced communicating compliance status in a checklist format.

Plan:

Next, I plan to integrate this compliance checklist into the organization's broader risk assessment framework and prepare all final documents for supervisor review.

Week 12– Reflective Journal Entry

Describe:

I wrapped up the internship by consolidating deliverables and participating in a final feedback session with my mentor. I organized project documentation, finalized checklists and reports, and received input on my overall performance.

Interpret:

This week helped me reflect on how much progress I made from OSINT investigations to framework mapping, report writing, and compliance analysis. Receiving detailed feedback helped me understand where I excelled and where I can still improve.

Evaluate:

I was proud to see how my outputs had evolved in quality and clarity. Time management and adaptability were key to completing everything on time. I appreciated the collaborative and flexible environment at Centropy.

Plan:

Moving forward, I plan to build on what I learned by studying cloud security in more depth, improving my technical toolset, and continuing to sharpen my documentation and reporting skills.

Work Samples

Work Sample 1: OSINT-Based Security Assessment for a Regional Healthcare Provider

During the early phase of my internship, I conducted a full Open-Source Intelligence (OSINT) cybersecurity assessment for a healthcare sector client. The aim of the assessment was to identify external exposures and vulnerabilities based solely on publicly available information, without any intrusive actions.

My responsibilities included passive reconnaissance of the organization's domains and subdomains using tools such as crt.sh, DNSDumpster, Shodan, and Amass. I analyzed the external hosting structure, technology stack, login portals, email configurations, and public

metadata associated with the client's digital assets. I also mapped all identified exposures to relevant NIST CSF functions and subcategories, helping to highlight areas needing risk mitigation and stronger governance.

Throughout the project, I prepared a structured technical report that included findings such as exposed WordPress login pages, username enumeration through error messages, missing security headers, outdated CMS versions, and the use of unsecured third-party services. Recommendations were provided for each finding, prioritizing actions based on risk severity and feasibility for a resource-constrained healthcare environment.

This work sample represents my skills in passive threat discovery, vulnerability analysis, cybersecurity framework mapping, and technical reporting in a professional context.

Attached Screenshots:

Below are selected anonymized screenshots showcasing the technical work completed during the OSINT-Based Cybersecurity Assessment for the healthcare sector client. Due to confidentiality agreements, all sensitive information such as domain names, IP addresses, organizational details, and user information has been redacted.

The screenshots represent a sample of the full report, which extended to over 17 pages and included:

- Enumeration of the organization's domain infrastructure and external hosting environment
- Analysis of publicly exposed systems and services
- Metadata leakage discovery from public documents
- Cloud storage exposure observations
- Technology stack analysis and identification of outdated components
- Risk categorization and security implications based on NIST CSF mapping

These examples illustrate the depth and breadth of the passive reconnaissance and risk assessment work conducted during the internship engagement.

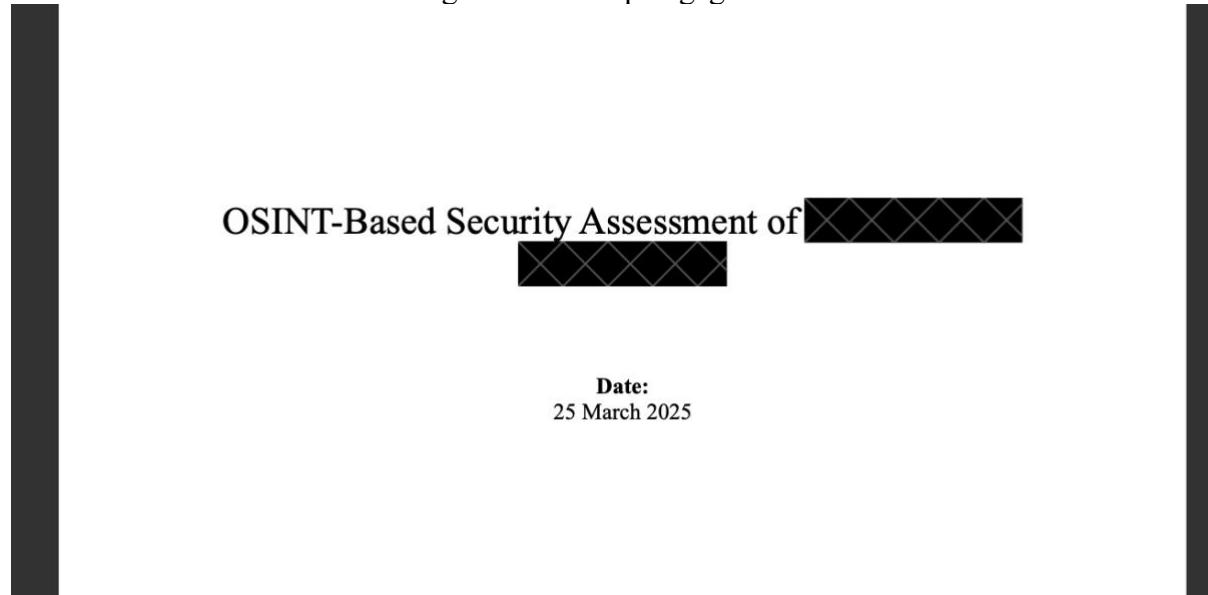
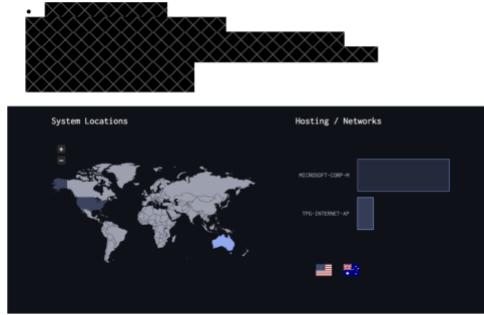


Figure 1

Table of Contents	
EXECUTIVE SUMMARY	3
COMPANY OVERVIEW.....	4
DOMAIN INFRASTRUCTURE.....	4
EMAIL INFRASTRUCTURE.....	6
ORGANIZATIONAL RELATIONSHIPS & SHARED INFRASTRUCTURE.....	7
CLOUD STORAGE OBSERVATION.....	8
TECHNICAL VULNERABILITIES.....	9
INFORMATION LEAKS AND EXPOSURE ANALYSIS.....	9
IDENTIFIED VULNERABILITIES AND SECURITY WEAKNESSES.....	11
1. Publicly Accessible WordPress Login Page	11
2. Username Enumeration via Login Error Messages	12
3. Valid Usernames Leaked in Sitemap	12
4. Outdated WordPress Version (3.9.7)	12
5. Contact Form 7 Plugin Usage	12
6. Lack of CAPTCHA or Rate Limiting on Login	12
7. No Two-Factor Authentication (2FA)	12
8. Archived robots.txt Discloses Internal Structure	12
9. Wildcard Domains	12
10. Subdomains Hosted on External Provider	12
11. Centralized Infrastructure Across Multiple Domains	13
12. Lack of DMARC reject Policy	13
13. Mixed Email Infrastructure	13
14. Use of Third-Party JavaScript Libraries	13
15. Use of Unsigned Third-Party Services	13
16. Missing HTTP Security Headers (assumed based on default config)	13
17. No Public Bug Reporting or Disclosure Policy	13
18. No Web Application Firewall on Subdomains	13
19. DNS TXT Records May Reveal Internal Integrations	13
20. Domain Type Risk	14
21. CNAME Dependencies for Core Functions	14
22. Missing Headers of Central Asset Inventory	14
COMPLIANCE GAPS AND EXPOSURE.....	14
NIST CYBERSECURITY FRAMEWORK MAPPING.....	15
APPENDIX.....	17

Figure 2

Company Overview:



Domain Infrastructure:

1. Domain Information



2. IP & Network Details



Though Microsoft owns the IP, it is likely leased to [REDACTED], indicating the use of Microsoft's cloud services.

Executive Summary

This report presents an Open-Source Intelligence (OSINT) assessment of the [REDACTED] and its associated digital infrastructure. The objective was to identify publicly accessible information that may reveal potential security weaknesses, misconfigurations, or exploitable vulnerabilities.

A comprehensive passive reconnaissance process was conducted, including DNS enumeration, infrastructure mapping, subdomain analysis, archive inspection, email authentication evaluation, and third-party integration review. No intrusive scanning or active exploitation was performed.

The investigation revealed 22 key vulnerabilities and weaknesses, ranging from technical misconfigurations to architectural risks. Notable findings include an exposed WordPress login page, username enumeration, leaked user identities via sitemap, outdated CMS version, missing security headers, and use of outdated or unverified plugins. Additionally, the domain is part of a centrally managed infrastructure shared across several hospital and healthcare-related domains, increasing the potential impact of lateral movement attacks.

Each weakness has been mapped to the relevant components of the NIST Cybersecurity Framework (CSF), highlighting specific control gaps in the Protect, Identify, Detect, and Respond functions. The majority of findings fall under the Protect and Identify functions, indicating a need for stronger access controls, patch management, asset inventory, and supply chain oversight.

This report provides a prioritized view of [REDACTED] from an attacker's perspective and offers actionable recommendations to reduce the organization's public attack surface and improve overall security posture.

3. DNS & Contact Information



4. Name Servers



Subdomain & DNS Enumeration

Discovered Subdomains



Wildcard Domain



Subdomain Hosting Info

macquarie[REDACTED].acurio.com.au



TXT Records (Security & Verification)



Figure 3



Figure 4



Figure 5

Work Sample 2: OSINT-Based Security Assessment for a Public Educational Institution

During the second phase of my internship, I conducted an Open-Source Intelligence (OSINT) assessment for a public educational institution. The objective was to identify vulnerabilities within the institution's external digital infrastructure through passive reconnaissance techniques, without performing any intrusive scanning activities.

My role involved mapping the organization's external footprint using tools such as Amass, crt.sh, DNSDumpster, and SecurityTrails. I focused on discovering subdomains, cloud storage exposure, login portals, outdated services, and publicly accessible administrative interfaces. Metadata analysis was performed on publicly available documents using tools like exiftool and mat2 to uncover hidden information that could assist attackers.

Throughout the project, I discovered and documented vulnerabilities such as exposed Plesk login panels, outdated JavaScript libraries, cloud storage misconfigurations, and missing authentication protections on public portals. Each finding was mapped to relevant subcategories of the NIST Cybersecurity Framework (CSF), allowing the risks to be prioritized and aligned with standard governance practices.

The findings and recommendations were compiled into a structured technical report aimed at supporting the client's risk mitigation efforts. This work sample highlights my technical capabilities in passive vulnerability discovery, risk analysis, NIST CSF alignment, and the preparation of professional cybersecurity assessment reports for client organizations.

Attached Screenshots:

Below are selected anonymized screenshots from the OSINT-Based Cybersecurity Assessment conducted for the public educational institution. All sensitive information, including domain names, IP addresses, and internal organizational references, has been carefully redacted to ensure confidentiality is maintained.

The screenshots demonstrate examples of:

- Subdomain enumeration and external infrastructure mapping
- Identification of public cloud storage exposures
- Detection of outdated or misconfigured technologies
- Metadata leakage analysis from publicly available documents
- Vulnerability documentation and mapping to NIST CSF controls

These samples are provided to illustrate the techniques and methods applied during the assessment, highlighting the real-world cybersecurity analysis skills developed during the internship.

Open-Source Intelligence (OSINT) Assessment Report
[REDACTED] – *External Exposure Analysis*

Prepared by: Tayyab Hameed
Master of Cybersecurity
April 2025

CONFIDENTIAL – For Internal Use Only. Unauthorized distribution is prohibited.

Figure6

1	Table of Contents	
2	Executive Summary.....	4
3	Introduction.....	4
4	Methodology.....	4
4.1	Reconnaissance Scope.....	4
4.2	Information Gathering Techniques.....	4
4.2.1	Public Data Sources & Intelligence Feeds.....	4
4.2.2	Non-Intrusive Surface Enumeration.....	5
4.2.3	Document & Metadata Analysis.....	5
4.2.4	Cloud Exposure & Configuration Analysis.....	5
4.3	Ethical Considerations.....	6
5	Organizational Overview.....	6
5.1	Institutional Background	6
5.2	Organizational Structure.....	6
5.3	Location & Campus	6
5.4	Public Affiliations & Government Oversight.....	7
5.5	Government Funding & Site Renewal Projects.....	7
6	Digital Footprint & Exposure Mapping.....	7
6.1	Identity & Access Management (IAM) Infrastructure.....	7
6.2	Subdomain & Infrastructure Enumeration.....	8
6.3	Website Technology Stack.....	8
6.3.1	Backend & Platform	8
6.3.2	Delivery & Infrastructure	8
6.3.3	Analytics & Marketing	9
6.3.4	Front-End Libraries & UX	9
6.3.5	Hosting Infrastructure & Service Providers	9
6.3.6	Login Portals & Public Services	10
6.3.7	Metadata & Document Storage Exposure	10
6.3.8	Robots.txt & Sitemap.xml.....	10
6.3.9	Directory & File Enumeration.....	11
6.3.10	Physical Intelligence (PHYSICALINT): Reconnaissance via Public Campus Maps.....	11
7	Vulnerability Breakdown	12
7.1	Exposed Plesk Login Panel	12
7.2	Public WordPress Login Panel (Main Domain)	13
7.3	Legacy WordPress Login Panel (Subdomain)	13
7.4	Dual-Authentication Surface on Paradigm Portal	14
7.5	Public AWS S3 Bucket with Predictable Document Paths	14
7.6	Metadata Exposure in Public Documents	15
7.7	Unused or Abandoned Subdomains	15
7.8	Use of Outdated JavaScript Libraries	15

CONFIDENTIAL – For Internal Use Only. Unauthorized distribution is prohibited.

CONFIDENTIAL – For Internal Use Only. Unauthorized distribution is prohibited.

Figure7

2 Executive Summary

This OSINT assessment identifies exposed digital assets, infrastructure misconfigurations, and publicly accessible resources related to the [REDACTED]. Key findings include a publicly exposed Plesk hosting panel, dual authentication surfaces, predictable document storage paths, metadata leakage, outdated JavaScript libraries, and several abandoned subdomains. These exposures present real risks of credential harvesting, phishing, privilege escalation, and reputational damage.

The report aims to provide visibility into [REDACTED] digital footprint and recommend practical mitigation strategies to reduce its external attack surface.

3 Introduction

This report presents an open-source intelligence (OSINT) assessment of the [REDACTED] conducted as part of a cybersecurity posture evaluation. OSINT techniques focus on publicly available data and passive reconnaissance to identify potential security weaknesses without engaging in intrusive actions.

The scope of this report includes domain enumeration, login portal exposure, metadata analysis of documents, subdomain discovery, and misconfiguration detection in cloud services and web technologies. The purpose is to highlight real-world attacker perspectives and offer risk-informed recommendations for mitigation.

4 Methodology

This OSINT assessment of the [REDACTED] was conducted using publicly accessible information and externally observable network behavior. The assessment was designed to simulate what a real-world attacker or external researcher could gather through open sources and indirect enumeration, without engaging in unauthorized access or system exploitation.

4.1 Reconnaissance Scope



4.2 Information Gathering Techniques

4.2.1 Public Data Sources & Intelligence Feeds

- **crt.sh:** Used to enumerate subdomains and certificate transparency logs.

CONFIDENTIAL – For Internal Use Only. Unauthorized distribution is prohibited.

- **SecurityTrails / DNSDumpster:** Leveraged for DNS structure mapping and domain history.

• **Search Engines & Google Dorks:**

- [REDACTED]
- [REDACTED]

• **Sitemap & Robots.txt Review:**

- [REDACTED]
- [REDACTED]

• **Archive Services:**

- [REDACTED]

4.2.2 Non-Intrusive Surface Enumeration

• **Subdomain Discovery:**

- Performed via Amass using public DNS records and certificate transparency data.

• **HTTP Path Enumeration:**

- Used dirsearch with conservative settings to identify whether standard config files or sensitive directories existed. Several returned 403 Forbidden, confirming their presence without accessing their contents.

• **Port and Service Discovery:**

- [REDACTED]

4.2.3 Document & Metadata Analysis

• **PDF and DOCX Metadata Extraction:**

- [REDACTED]

• **File Naming & Structure Analysis:**

- [REDACTED]

4.2.4 Cloud Exposure & Configuration Analysis

• **S3 Bucket Structure:**

- Public URLs were tested for predictable access using folder and file naming patterns, with access denied pages confirming structure existence.
- Bucket permissions and file access paths were assessed for potential overexposure.

CONFIDENTIAL – For Internal Use Only. Unauthorized distribution is prohibited.

Figure8



CONFIDENTIAL – For Internal Use Only. Unauthorized distribution is prohibited.

CONFIDENTIAL – For Internal Use Only. Unauthorized distribution is prohibited.

Figure9

Work Sample 3: Phishing Incident Identification and Analysis Report

During the course of my internship, I encountered a real-world phishing attack impersonating a senior executive from Centropy Services & Solutions. Upon recognizing suspicious patterns in the email, including the use of a public domain and urgency tactics, I escalated the incident to my supervisor through the proper internal reporting channels. I was subsequently assigned to perform a detailed technical analysis of the phishing email as a side project.

In this task, I conducted a full forensic review of the email headers, routing information, IP origin tracing, and language content analysis. Using tools like WHOIS lookups and email source examination, I identified that the email originated from a public Mail.ru domain and was part of a Business Email Compromise (BEC) attempt targeting financial exploitation through gift card scams.

The final deliverable was a Phishing Email Analysis Report which documented the timeline of attacker communication, technical header data, source analysis, and social engineering techniques employed. The report also included actionable recommendations for mitigating future phishing threats, including verification protocols and staff awareness improvements.

This work sample demonstrates my skills in real-world incident handling, phishing analysis, technical report writing, and the application of social engineering defense principles within a professional cybersecurity context.

Attached Screenshots:

Screenshots of the phishing email headers, timeline of attacker communication, IP address WHOIS results, and forensic analysis summaries are included below to illustrate the investigative work performed.

Phishing Email Analysis Report
Business Email Compromise (BEC) Attempt: Gift Card Scam via
Executive Impersonation

Date of Incident:
31 March 2025

Prepared by: Tayyab H

Table of Contents

EXECUTIVE SUMMARY.....	3
TIMELINE OF EVENTS.....	3
EMAIL HEADER & SOURCE ANALYSIS.....	3
IP ADDRESS ORIGIN ANALYSIS.....	4
LANGUAGE & CONTENT ANALYSIS.....	5
ATTACK OBJECTIVE & METHODOLOGY.....	6
CONCLUSION.....	6
APPENDIX.....	7

Executive Summary

This report analyses a targeted phishing attempt against Tayyab H, a cybersecurity intern at Centropy Services & Solutions, a Sydney-based consultancy firm. The attacker impersonated *Varun N. Batra*, a senior executive at the firm, and initiated contact shortly after the intern joined the organization in February 2025, a period where new employees are often more vulnerable to trust-based social engineering.

The phishing email was carefully crafted to create urgency and emotional pressure, claiming the need to buy four Apple gift cards worth \$500 each as part of a confidential surprise for staff. The attacker exploited the victim's presumed eagerness to assist senior leadership, aiming to manipulate him into a fraudulent financial transaction.

However, due to prior knowledge of phishing tactics and cybersecurity awareness, the intern quickly identified red flags, including the use of a public domain email (`mail.ru`), the informal tone, urgency, and lack of verification. The email was promptly flagged, and the real Varun Batra was contacted via official channels. No loss occurred.

This report documents the full communication, header analysis, and forensic review of the phishing email's route and infrastructure. It serves as a valuable case study for understanding how Business Email Compromise (BEC) scams exploit trust, timing, and urgency and how cybersecurity training plays a critical role in defending against such attacks.

Timeline of Events

Time	Event Description	Reference
09:52 AM	Attacker (impersonating Varun Batra) sends an email asking if I am available.	Screenshot 1
11:44 AM	I respond confirming my availability via email.	Screenshot 2
11:48 AM	Attacker asks for confidential assistance for a surprise gift for staff.	Screenshot 3
11:52 AM	Attacker tries to build trust, says "I trust your reliability."	Screenshot 4
12:04 PM	Follow-up message sent by attacker due to no immediate action.	Screenshot 5
12:10 PM	Specific request made: 4 Apple gift cards, \$500 each.	Screenshot 6
12:11 PM	Attacker instructs to scratch and email the codes, claiming reimbursement later.	Screenshot 7
12:19 PM	More pressure: Attacker asks, "can I get it now?"	Screenshot 8
~12 PM	I identify red flags and report the incident to the real Varun via work email.	Screenshot 9

Email Header & Source Analysis

This section presents a technical analysis of the phishing email, its routing path, and metadata to assess sender authenticity and identify red flags.

Summary of Email Header:

Prepared by: Tayyab H

Figure10

- Subject: Khan Tayyab
- Message-ID: <1743375155.518743445@f477.i.mail.ru>
- Creation Time: Mon, 31 Mar 2025 01:52:35 +0300
- Delivered After: 22 seconds
- From: Varun N. Batra <j190473773@mail.ru>
- Reply-To: Same as sender
- To: tayyabtavv@gmail.com, khan_tayyab57@yahoo.com

Email Routing Path (Received Hops):

Hop #	Server/Service	Protocol/Method	Date & Time	Delay
1	e.mail.ru	HTTP	31 Mar 2025, 09:52:35	-
2	f747.i.mail.ru	Local	31 Mar 2025, 09:52:36	1 sec
3	From 45.84.129.118 → 10.197.34.205	SMTPs (TLS1.2)	31 Mar 2025, 09:52:57	21 sec
4	From 10.197.34.205 → Yahoo Server	HTTPS	31 Mar 2025, 09:52:57	0 sec

Authentication & Delivery Results:

- Sender Domain: mail.ru (public/free domain)
- X-Originating-IP: 45.84.129.118 (*external and non-corporate*)
- SPF (Sender Policy Framework): *Pass*
- DKIM (DomainKeys Identified Mail): *Pass*
- DMARC (Domain-based Message Authentication): *Pass*
- Final Destination: khan_tayyab57@yahoo.com at 22:52:57 UTC

Although the email passed SPF, DKIM, and DMARC, the use of a public domain (mail.ru) and non-corporate origin IP address are strong red flags suggesting this was a legitimate-looking email from an attacker-controlled account.

IP Address Origin Analysis

A WHOIS lookup was conducted on the originating IP address 45.84.129.118, which appeared in the email header (X-Originating-IP). The IP falls under the network range 45.84.128.0 - 45.84.129.255 and is assigned to VK Services, a Russian company formerly operating Mail.ru infrastructure.

WHOIS Findings:

- IP Address: 45.84.129.118
- Network Owner: VK Services (Mail.ru Group)
- Organization: Limited Liability Company VK
- Country: Russia (RU)
- Netname: VK-FRONT
- Abuse Contact: abuse@corp.mail.ru
- Address: Leningradskiy Prospect 39/79, Moscow, 125167 Russia
- Maintainer: VKCOMPANY-MNT
- Phone: +7 495 7256357

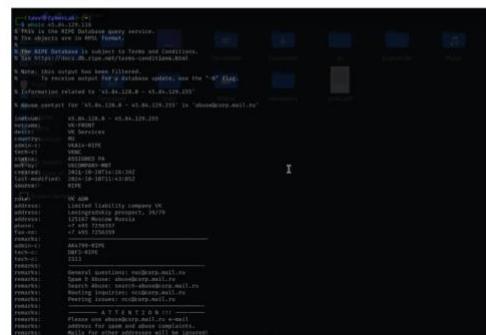
The IP address is registered to VK (formerly Mail.ru), a Russian tech company. Although the message passed SPF/DKIM checks, the use of a personal Mail.ru address and origin from this public infrastructure confirms the sender is external and untrusted. The attacker likely used

Prepared by: Tayyab H

Figure11

Mail.ru's free email service to craft a legitimate-looking message, exploiting trust and authority.

Whois 45.84.129.118



Language & Content Analysis

The phishing email used a formal but overly simplistic tone to establish trust and urgency. The attacker began with a vague question, "Do you have any spare time right now via email?", which is a common tactic in social engineering to initiate conversation without triggering suspicion.

The tone throughout was polite and seemingly respectful, using phrases such as "*I trust your reliability on this*", but this was clearly manipulative, aiming to create a sense of responsibility in the target.

There were several language and structure-based red flags:

- No company email signature or branding.
- The sender asked the intern to "*keep this confidential*", a psychological trick to isolate the victim.
- The attacker asked for a non-standard financial transaction (Apple gift cards) without using any official procurement or documentation process.

Prepared by: Tayyab H

- Phrases like “*You’ll be reimbursed later*” are highly suspicious and often used in gift card scams.
- The request came from a public Mail.ru domain rather than a verified corporate address, breaking normal business communication norms.

Despite the email passing technical authentication (SPF, DKIM), its linguistic and structural elements strongly indicate deception, supporting its classification as a phishing attempt.

Attack Objective & Methodology

The phishing attempt analysed in this report is a Business Email Compromise (BEC) scam, specifically designed to extract monetary value in the form of Apple gift cards. The attacker impersonated a senior executive from Centropy Services & Solutions (Varun N. Batra) and targeted a recently joined intern, assuming lower familiarity with internal communication protocols and chain of command.

Attack Objective:

To trick the target into:

- Purchasing four Apple gift cards worth \$500 each.
- Sending back the card numbers and PINs via email.
- Using personal funds under the promise of later reimbursement.

Methodology Used:

1. Impersonation: Used the name of a real senior executive (Varun N. Batra) to build authority.
2. Trust Exploitation: Targeted a new intern, assuming they’d be more willing to assist.
3. Urgency & Secrecy: Claimed the task was “confidential” and “urgent,” intended as a surprise for employees.
4. Social Engineering: Used polite, flattering language to gain compliance (“I trust your reliability”).
5. Public Email Domain: Sent the email from a mail.ru address instead of an official company domain to avoid internal detection.

Conclusion

This report documented a real-world phishing attempt involving impersonation, social engineering, and financial fraud targeting a new cybersecurity intern at Centropy Services & Solutions. The attacker leveraged the identity of a senior executive, urgency, and emotional manipulation to pressure the target into purchasing and sending high-value Apple gift cards.

Through timely observation, familiarity with phishing tactics, and proper verification, the attack was promptly detected and neutralized without financial loss. This incident highlights the importance of continuous phishing awareness, especially for new hires, and the need for strong internal communication protocols to defend against Business Email Compromise (BEC) threats.

Prepared by: Tayyab H

Figure12

Appendix

Screenshot 1

From: Varun N. Batra <j190473773@mail.ru>
Date: Monday, 31 March 2025 at 09:52
To: tayyabtavv@gmail.com <tayyabtavv@gmail.com>, khan_tayyab57@yahoo.com <khan_tayyab57@yahoo.com>
Subject: Khan Tayyab

Hello
Do you have any spare time right now via email ?
Looking forward to hearing from you soon.

BEST REGARDS,
Varun N. Batra

Screenshot 2

TK Tayyab Khan
To: Varun - Mon, Mar 31 at 10:44 AM

Hi, Yes I'm available.

Screenshot 3

VB Varun N. Batra
To: me, and 1 other - Mon, Mar 31 at 10:48 AM

I need you to handle a request for me.
Kindly let me know if you are available right now.
Hide trimmed content ▾

BEST REGARDS,
Varun N. Batra

Prepared by: Tayyab H

Screenshot 4

VB Varun N. Batra
To: me, and 1 other - Mon, Mar 31 at 11:52 AM

Okay Khan
Here is what I want you to do for me - because I'm a little bit busy right now.
I have been working on some incentives and I am surprising some of our diligent staffs with gifts today.
This should be confidential until they all have the gift as it's a surprise.
Let me know if you can take care of this, so I'll send the rest of the details.
Show trimmed content ▾

Screenshot 5

VB Varun N. Batra
To: me, and 1 other - Mon, Mar 31 at 12:04 PM

Hello Khan
Can you handle that for me
Show trimmed content ▾

Screenshot 6

TK Tayyab Khan
To: Varun - Mon, Mar 31 at 12:05 PM

what is it ?
-

Screenshot 7

VB Varun N. Batra
To: me, and 1 other - Mon, Mar 31 at 12:10 PM

good Khan,
The errand in question is relatively simple and should not take up too much of your time. I trust your reliability and attention to detail, which is why I felt comfortable in reaching out to you for assistance. I understand that your own schedule may be busy as well, but your support would truly ease my workload significantly, am so sorry for the inconvenience that this may put you. I am so glad I could count on you in getting this done for me, I will be glad if you can help get it done now. I need 4 qty of Apple gift cards \$500 on each (total \$2000) you should get them from any store around you
Show trimmed content ▾

Screenshot 8

VB Varun N. Batra
To: me, and 1 other - Mon, Mar 31 at 12:11 PM

I intend to surprise the staffs with the picture of the gift cards through their emails respectively. Kindly scratch off the back of each gift card, take a clear picture of each gift card back and send them to me here once you have them. I will handle the disbursement myself, I'll recommend you purchase them in multiple stores if there's a limit.
kindly fund this purchase with your personal card, and I'll have you reimbursed Asap.
Please keep the physical cards and receipt for reference and also for any additional cost incurred. Thanks.
Show trimmed content ▾

Screenshot 9

VB Varun N. Batra
To: me, and 1 other - Mon, Mar 31 at 12:19 PM

Hi Khan
How soon can you get it done
Show trimmed content ▾

Prepared by: Tayyab H

Figure13

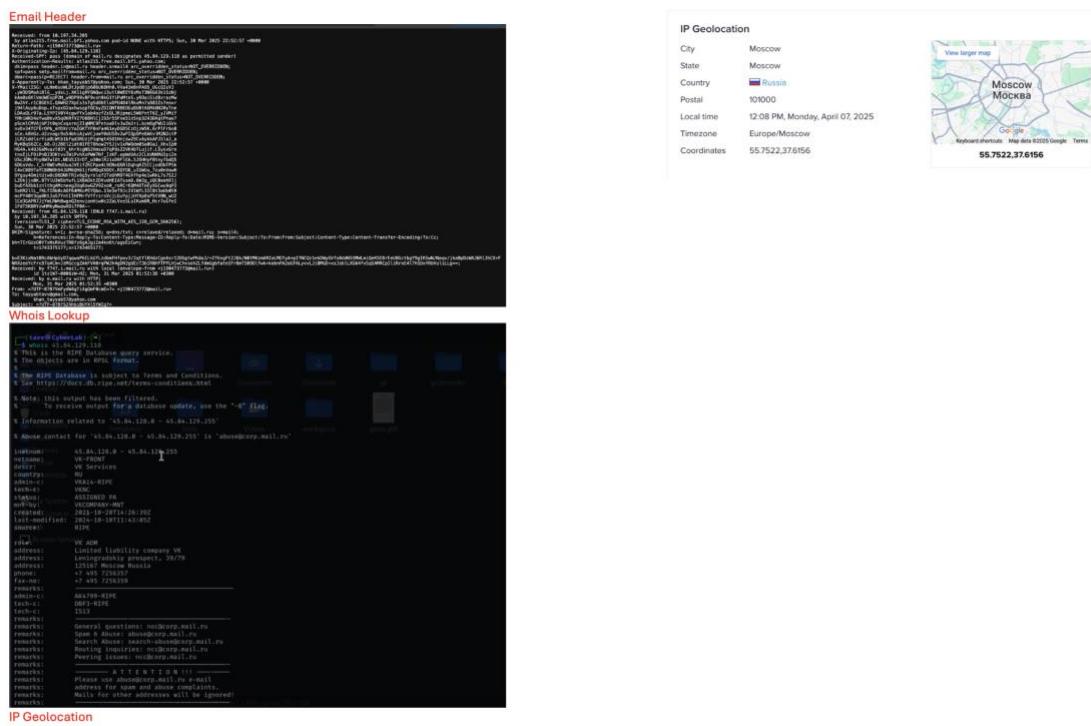


Figure 14

Critical Analysis

This critical analysis reflects on the complete duration of my internship at Centropy Services & Solutions, spanning thirteen weeks from late February to the end of May. The experience provided a deep immersion into the day-to-day responsibilities of a cybersecurity consultant, blending technical tasks with strategic thinking and communication. My role evolved over time, starting with open-source intelligence (OSINT) investigations and vulnerability analysis, and gradually moving into framework alignment, compliance mapping, and the creation of practical implementation resources for clients.

The foundation I had built through university coursework played an important role in helping me navigate the early stages of the internship. Concepts such as the NIST Cybersecurity Framework (CSF), incident response planning, and risk categorization were not entirely new to me. However, applying these concepts in a real client-facing environment was a very different challenge. I learned that frameworks are not applied rigidly. Instead, they need to be interpreted based on the client's size, maturity, regulatory obligations, and risk tolerance.

One of the most significant lessons I learned early on was that information gathering through OSINT is not about simply running a few tools and collecting results. It requires critical thinking to filter meaningful data from irrelevant noise. I had to decide which vulnerabilities or exposures were worth reporting and understand how different findings could combine to create broader attack paths. For example, a misconfigured login page or an unprotected cloud bucket may seem minor in isolation, but in the context of an organization with limited monitoring capabilities, they could represent serious risks.

Midway through the internship, I was given the opportunity to contribute to more strategic components of cybersecurity assessments. This included mapping vulnerabilities to NIST CSF

subcategories, identifying gaps in the control environment, and helping develop tailored remediation steps. This phase was particularly challenging because it required translating technical observations into clear, actionable recommendations that would be understood and implemented by stakeholders who may not have deep technical expertise. It helped me practice switching between technical detail and business-focused communication, which I now see as one of the most valuable skills in cybersecurity consulting.

In the later weeks of the internship, I shifted focus toward developing internal tools and compliance resources. One of the highlights of this phase was creating a cybersecurity posture assessment questionnaire designed for small and mid-sized organizations. I structured it around core themes such as identity and access management, incident response, and data protection, using language that was simple but accurate. I tested the questionnaire using a masked organization and received feedback that helped improve its clarity and relevance. This experience taught me that tools are most effective when they balance thoroughness with usability.

I also had the chance to explore regulatory compliance by working on a checklist aligned with the Digital Operational Resilience Act (DORA), which was a new area for me. This task required me to interpret regulatory language and translate it into specific control requirements and evidence expectations. It helped me understand how organizations prepare for audits and how policy-level decisions shape technical practices. Working with DORA deepened my appreciation for the role of compliance in cybersecurity and the value of frameworks that link governance with day-to-day controls.

Throughout the internship, there were several challenges that contributed to my learning. Time management was a consistent theme, especially in a hybrid work environment where I was responsible for setting my own pace. There were times when I spent too long perfecting individual sections of a report or cross-validating OSINT findings, only to realize I needed to allocate more time to presentation and refinement. With support from my mentor, I learned to establish clearer timelines, create daily goals, and prioritize deliverables based on impact and deadlines.

Another challenge was in professional communication. Writing reports for a client audience was very different from academic writing. I had to learn how to present technical content in a way that highlighted relevance, risk, and actionability. Initially, I tended to include too much technical jargon or over-explain findings. Through feedback and review sessions, I gradually developed a writing style that focused on clarity, structure, and business relevance. I now feel more confident communicating with both technical and non-technical audiences.

A unique and unexpected learning moment came when I encountered a phishing email impersonating a senior executive. I recognized the indicators of compromise and escalated it appropriately. Later, I was asked to perform a detailed analysis of the email's tactics, source, and intent. This hands-on incident helped reinforce concepts I had studied theoretically, such as social engineering, email header analysis, and business email compromise tactics. It also demonstrated the importance of vigilance and a structured response process.

Looking back, I believe this internship helped me grow not only in technical capability but also in critical thinking, professional communication, and adaptability. I am now much more comfortable conducting end-to-end assessments, from information gathering and vulnerability analysis to control mapping and client reporting. I have also begun to develop a cybersecurity mindset—one that is proactive, context-aware, and always thinking in terms of both threats and mitigations.

In terms of areas for future development, I recognize the need to strengthen my technical expertise in cloud security. While I encountered cloud misconfigurations during OSINT investigations, I realized that I lacked the deeper understanding of AWS, Azure, or Google

Cloud configurations necessary to perform more advanced assessments. I plan to pursue additional learning in this space, through both certifications and hands-on labs.

I am also interested in enhancing my forensic investigation skills. The phishing report gave me a glimpse into email analysis and threat tracing, but I know there is much more to learn in terms of log analysis, endpoint forensics, and malware reverse engineering. These are areas I would like to explore further, possibly through structured training or real-world incident handling exercises.

Lastly, I aim to continue improving my ability to assess risk in a structured way. While I made progress during the internship, I sometimes found it difficult to weigh technical severity against business impact. I plan to study frameworks such as FAIR and look at real case studies to develop better judgment in prioritizing threats and controls.

In conclusion, the internship was an important milestone in my professional development. It helped me move from theoretical understanding to practical application, exposed me to real client challenges, and sharpened my ability to think like both a security analyst and a consultant. I leave the experience with greater confidence, a clearer direction, and a deeper commitment to growing as a cybersecurity professional.

SWOT Analysis

This section presents a SWOT analysis of Centropy Services & Solutions, the organization where I am currently completing my cybersecurity internship. Centropy is a boutique cybersecurity consultancy firm based in Sydney, Australia, specializing in Governance, Risk, and Compliance (GRC) services. The firm provides advisory, assurance, and managed cybersecurity services to small and medium-sized enterprises across various sectors including healthcare, education, and professional services. This analysis evaluates the internal strengths and weaknesses of the organization, as well as the external opportunities and threats it faces within the evolving cybersecurity market.

Strengths

Centropy Services & Solutions has several internal strengths that contribute to its success as a cybersecurity consultancy firm. One of the most significant strengths is its specialization in Governance, Risk, and Compliance (GRC) services. Unlike broader technology companies that offer a wide range of IT services, Centropy focuses specifically on cybersecurity risk management, compliance frameworks, and security governance. This focused expertise allows the company to position itself as a trusted advisor for organizations that require structured, framework-based cybersecurity solutions.

Another major strength is the quality and experience of its leadership and consulting team. Senior executives at Centropy bring extensive industry experience from both technical and governance backgrounds, allowing the firm to bridge the gap between technical cybersecurity controls and business-driven security governance. This balanced expertise enhances Centropy's credibility with clients and allows it to deliver actionable, risk-prioritized advice rather than theoretical recommendations.

Centropy's boutique structure is also an advantage. With a small, agile team, the company can offer highly personalized services to its clients. Clients are often able to work directly with senior consultants rather than dealing with large account management hierarchies common in bigger firms. This high-touch engagement model increases client satisfaction and loyalty, particularly among small and medium-sized businesses that value close working relationships.

Flexibility and adaptability are additional internal strengths. Centropy is able to tailor its services based on the specific needs, maturity levels, and budgets of its clients. Whether clients require full cybersecurity risk assessments, gap analyses against NIST CSF or ISO 27001, or assistance with Essential Eight compliance, Centropy can adapt its methods accordingly without applying rigid, one-size-fits-all approaches.

Finally, Centropy's emphasis on practical, implementable solutions rather than overcomplicated theoretical models gives it an advantage, especially when working with smaller organizations that need cost-effective and realistic cybersecurity improvements. This client-centered approach strengthens its reputation and helps in building long-term trusted advisory relationships.

Weaknesses

Despite its many strengths, Centropy also faces some internal weaknesses that could limit its growth or ability to compete with larger firms. One major weakness is its relatively small team size. While the boutique model offers personalized service, it also limits the firm's ability to scale operations quickly when dealing with multiple clients simultaneously or when responding to large project demands. Resource constraints can make it challenging to deliver on tight deadlines or take on high-volume consultancy projects.

Another internal weakness is limited brand recognition. Compared to larger cybersecurity consulting firms like Deloitte, PwC, or KPMG, Centropy has a smaller public presence. This can sometimes make it harder to attract larger enterprise clients who often prefer to work with well-known firms for regulatory reporting or board-level advisory services.

Centropy's reliance on a limited range of core services could also be seen as a weakness. While specializing in GRC is a strength, it also narrows the potential client base. Organizations looking for broader managed security services, such as Security Operations Center (SOC) outsourcing or offensive security testing, may turn to firms with a wider service portfolio.

Additionally, the firm's reliance on a small group of key personnel can introduce operational risk. If senior consultants leave, the company could face knowledge gaps, project delays, or even client relationship issues. Unlike larger firms with distributed resources and backup teams, boutique firms must carefully manage knowledge transfer and succession planning.

Finally, Centropy's marketing and online visibility could be improved. In an increasingly competitive cybersecurity consulting market, a strong digital presence, thought leadership content, and visible client success stories are important for brand building. Currently, Centropy's online footprint is limited, which could affect its ability to reach new prospects in competitive bidding situations.

Opportunities

Centropy has several external opportunities it can leverage to grow its business and strengthen its position in the cybersecurity consulting market. One of the biggest opportunities is the overall increase in cybersecurity awareness across industries. Small and medium-sized businesses, which were previously slow to invest in cybersecurity, are now recognizing the importance of frameworks like Essential Eight, ISO 27001, and the NIST Cybersecurity

Framework. This creates a strong demand for advisory services that Centropy is well positioned to deliver.

Another major opportunity comes from regulatory developments. Government bodies and industry regulators are introducing stricter cybersecurity compliance requirements. For example, Australian regulations now require mandatory breach notifications and risk assessments for certain sectors. Centropy's expertise in governance and compliance consulting allows it to help clients navigate these regulatory changes effectively.

The shift to cloud services among businesses also opens new opportunities for Centropy. Many organizations are migrating to platforms like AWS, Microsoft Azure, and Google Cloud, but struggle with cloud security configurations. Centropy can expand its services by offering cloud risk assessments and security posture evaluations tailored to small and medium-sized businesses.

There is also an opportunity to differentiate by providing specialized training and awareness services. As social engineering attacks such as phishing continue to rise, many organizations need practical training for their employees. Given Centropy's experience with real-world phishing cases and risk management, launching security awareness programs could open a new service stream.

Finally, Centropy could explore partnerships with Managed Service Providers (MSPs) and cybersecurity product vendors to offer bundled services. Strategic alliances can help the company expand its service offerings without the need to invest heavily in building full technology delivery teams.

Threats

Despite the available opportunities, Centropy also faces several external threats that could impact its growth and stability. One of the main threats is competition from larger cybersecurity consulting firms. Companies like Deloitte, PwC, and BDO have much larger resource pools, global brand recognition, and the ability to offer end-to-end cybersecurity solutions. These larger firms may dominate the market for larger enterprises and high-profile projects, limiting Centropy's ability to scale beyond the small and medium-sized business sector.

Another significant threat is the rapidly changing cybersecurity landscape. As new threats emerge, cybersecurity consultancies must continuously update their methodologies, tools, and knowledge bases. Falling behind in threat intelligence, emerging technology risks (such as IoT security, AI-driven attacks, or cloud-native vulnerabilities) could impact Centropy's competitiveness.

Economic uncertainty is also a potential threat. During economic downturns, many small and medium-sized businesses cut discretionary spending, and cybersecurity consulting services could be deprioritized. As Centropy's client base consists largely of smaller organizations, an economic slowdown could reduce demand for its advisory services.

The growing trend of cybersecurity automation is another external threat. Tools that automate compliance assessments, vulnerability management, and risk reporting are becoming more accessible. Organizations might choose automated solutions over boutique consultancy services for cost reasons, particularly at the lower end of the market.

Lastly, changes in regulatory requirements could pose a challenge if Centropy does not invest in ongoing training and adaptation. As compliance standards evolve, consultancies must be able to interpret and implement new frameworks rapidly. Falling behind in knowledge or failing to deliver updated services could erode client trust and lead to lost business.

Conclusion

Reflecting on the full scope of my internship at Centropy Services & Solutions, I gained not only technical exposure but also a deeper appreciation for the role of cybersecurity advisory in real-world environments. The experience allowed me to apply my academic knowledge in practical settings, from conducting OSINT investigations and mapping vulnerabilities to frameworks like the NIST CSF, to developing mitigation roadmaps, compliance checklists, and posture assessment tools.

Centropy's strength lies in its focused expertise in Governance, Risk, and Compliance, especially in delivering tailored, actionable security advice for small and mid-sized organizations. I saw how the firm's practical and flexible approach, combined with its client engagement model, allows it to deliver meaningful results without overwhelming clients with theoretical complexity.

The final phase of my internship provided opportunities to work on internal assets such as a cybersecurity questionnaire and a DORA compliance checklist. These activities helped me understand the importance of making security understandable and manageable for clients, especially those with limited internal resources or technical expertise.

I also observed some of the challenges a boutique consultancy can face. While Centropy's small team and agile methods are a clear strength, they also present limitations in terms of scalability, visibility, and resourcing for larger engagements. At the same time, the growing demand for cybersecurity services, increased regulatory scrutiny, and digital transformation efforts across industries provide Centropy with many opportunities for expansion and specialization.

Overall, the internship was a valuable bridge between theory and practice. I had the chance to work independently, contribute to real client-facing work, and receive mentorship from experienced professionals. It also gave me a clear understanding of how cybersecurity is implemented in organizations and how communication, clarity, and practicality are just as important as technical depth. This experience has strengthened my interest in advisory and GRC work and will help guide my future development as I continue to build both my technical skills and strategic understanding of cybersecurity.

Recommendation

Based on the insights gathered throughout the internship, along with the observations shared in the critical analysis and SWOT evaluation, I would like to offer several recommendations that could help Centropy Services & Solutions continue its growth and build resilience in a competitive market.

To begin with, Centropy could benefit from expanding its delivery capacity through a scalable associate consultant model. Given the firm's lean team size, forming structured partnerships with trusted freelance consultants or boutique firms would enable it to take on larger or parallel engagements without stretching internal resources. This approach could preserve quality while also introducing greater flexibility when managing fluctuating workloads.

The company would also benefit from a more deliberate investment in its online brand presence. While Centropy is well regarded by its clients, it could improve visibility by sharing anonymized case studies, blogs, and white papers. Highlighting its niche expertise in GRC and practical cybersecurity frameworks—especially through platforms like LinkedIn, industry webinars, or cybersecurity forums—could enhance credibility and attract higher-profile engagements.

Another opportunity lies in gradually expanding Centropy's service offerings. While its focus on cybersecurity advisory and compliance is a strength, integrating adjacent services such as cloud security posture reviews, user awareness training, or lightweight security operations advisory could meet more of the evolving needs of small and mid-sized businesses. This could also diversify revenue streams while remaining within the scope of the firm's strategic strengths.

In terms of operations, formalizing internal documentation and knowledge management would be valuable. Developing a central repository of reusable templates, control checklists, and engagement methodologies would reduce the firm's reliance on key individuals and support smoother onboarding of new team members or partners.

Given the growing presence of automated compliance and risk management platforms, Centropy should explore selectively integrating automation into its workflows. Tools that assist with vulnerability scanning, report generation, or policy documentation could increase efficiency without diluting the firm's personalized service model.

Lastly, continued professional development for internal staff should remain a top priority. As cybersecurity threats and compliance standards evolve rapidly, structured training plans can ensure the team remains up to date. Exposure to new frameworks like DORA, advances in cloud security, and regulatory changes could further enhance Centropy's ability to deliver high-value, relevant advisory services.

In summary, Centropy's strong technical foundation and client-focused model are well suited to the needs of modern businesses. By investing in scalability, visibility, service breadth, and internal process maturity, the organization can further strengthen its position as a trusted cybersecurity partner in an increasingly complex and regulated digital landscape.

References:

Australian Cyber Security Centre. (2021). *The Essential Eight explained*. Australian Government. <https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-explained>

Australian Digital Health Agency. (2019). *Cyber security centre resources*. <https://www.digitalhealth.gov.au/about-us/digital-health-cyber-security-centre>

CompTIA. (2015). *Security+ (Plus) certification | CompTIA IT certifications.* <https://www.comptia.org/certifications/security>

crt.sh. (n.d.). *Certificate transparency log search.* <https://crt.sh/>

DNSDumpster. (n.d.). *Online DNS reconnaissance tool.* <https://dnsdumpster.com/>

Gill, R. (2023, February 23). *What is OSINT (Open-source intelligence)?* SANS Institute. <https://www.sans.org/blog/what-is-open-source-intelligence/>

Harvey, P. (n.d.). *ExifTool metadata extraction tool.* <https://exiftool.org/>

International Organization for Standardization. (2013). *ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements.* <https://www.iso.org/standard/54534.html>

Microsoft Corporation. (n.d.). *What is business email compromise (BEC)?* <https://www.microsoft.com/en-au/security/business/security-101/what-is-business-email-compromise-bec>

National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity* (Version 1.1). <https://doi.org/10.6028/NIST.CSWP.04162018>

National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (Version 2.0). <https://doi.org/10.6028/nist.csfp.29>

Office of the Australian Information Commissioner. (2023, March 10). *Data breach preparation and response.* <https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/preventing-preparing-for-and-responding-to-data-breaches/data-breach-preparation-and-response>

OWASP Foundation. (2024, September). *OWASP Top Ten.* <https://owasp.org/www-project-top-ten/>

SecurityTrails. (n.d.). *The world's largest repository of historical DNS data.* <https://securitytrails.com/>

Shodan. (n.d.). *Explore the internet of things with Shodan.* <https://www.shodan.io/>

Mitre Corporation. (n.d.). MITRE ATT&CK® Framework. Retrieved from <https://attack.mitre.org/>

National Institute of Standards and Technology. (2021). Digital Identity Guidelines (SP 800-63-3). <https://pages.nist.gov/800-63-3/>

Amazon Web Services. (n.d.). AWS Cloud Security Best Practices. <https://docs.aws.amazon.com/whitepapers/latest/aws-security-best-practices/aws-security-best-practices.pdf>