Reflection on UX Design Process: TRADIE Cybersecurity Incident Response Prototype

Marco Giacoppo
School of Computer Science
Swinburne University of Technology
Melbourne, Australia
104071453@student.swin.edu.au

***Abstract*—This paper reflects on the process of developing a user interface prototype for the Tasmanian Regional Agency for Digital Innovation and Ethics (TRADIE). The prototype addresses cybersecurity incident reporting, workflow management, and compliance requirements. The report discusses the design thinking process, collaborative and independent learning experiences, project management strategies, and ethical considerations under the Australian Computer Society's (ACS) Code of Professional Conduct.**

***Index Terms*—UX Design, Reflection, Cybersecurity, Incident Response, Design Thinking, ACS Ethics, Project Collaboration**

I. Introduction

This report presents my personal reflection on the user interface prototype project conducted for the Tasmanian Regional Agency for Digital Innovation and Ethics (TRADIE). The project aimed to address TRADIE's growing concerns around cybersecurity incident management and compliance, particularly in relation to the deployment of an on-premise email server and the broader cyber threat landscape.

Working as part of a five-member team, our objective was to design and prototype a user-centered digital interface that enables staff to report cybersecurity incidents, allows administrators to verify email server compliance, and empowers the Information Security Officer (ISO) to manage threats effectively in alignment with the Australian Signals Directorate's *Cyber Security Incident Response Planning: Practitioner Guidance* (Australian Signals Directorate, 2022).

Throughout the semester, we applied design thinking principles to guide our user research, ideation, prototyping, and testing. Tools like Confluence, Jira, Discord and Figma enabled us to collaborate efficiently, manage sprint tasks, and refine the prototype based on stakeholder feedback. Our team also maintained regular stand-ups, retrospectives, and documentation through Confluence to ensure transparency and structured progress.

As the Product Owner and co-developer, I played a significant role in aligning the prototype with TRADIE's core needs. This paper reflects on my individual contributions, key lessons learned, and how this project helped me grow as both a designer and a collaborator, while adhering to ethical and professional standards outlined by the Australian Computer Society (ACS).

II. Design Thinking and UX Process

Our team followed a user-centered design thinking approach, consisting of five phases: empathise, define, ideate, prototype, and test (Brown, 2009). This method helped us stay grounded in the needs of different user roles while aligning our solution with TRADIE's cybersecurity response objectives.

In the *empathise* phase, we created five distinct personas: Alex (Information Security Officer), Sarah (communications staff), William (administrative officer), Emily (graphic designer), and David (program coordinator). These personas were developed using role-based assumptions and research into common pain points across public sector cybersecurity training and incident reporting. For instance, Alex required structured reporting and incident logs, while Sarah and William needed a simplified, non-technical interface. Our empathy maps and user journey flows highlighted barriers such as hesitation to report suspicious activity, unclear escalation channels, and lack of progress tracking.

During the *define* phase, we refined our problem statement to: "Design a secure, accessible, and role-specific interface that enables effective cyber incident reporting, compliance tracking, and readiness evaluation." Journey maps helped us visualize how users moved through the system — for example, how Sarah might report a suspected phishing attempt and expect a status update, or how the ISO reviews trends via the dashboard.

In the *ideate* phase, we held brainstorming sessions using Miro and card sorting exercises to prioritize features. We generated user stories (e.g., "As a staff member, I want to report an incident in less than 2 minutes") and wireframed ideas like the 'Report Incident' form and threat filters. This led to design decisions such as adding helper icons for non-technical users and providing dropdowns for selecting threat types.

The *prototype* was developed in Figma, with separate panels for Admin, ISO, and general staff. Key screens included:

- A step-by-step incident report form with dropdowns and tooltips
- The "My Courses" page to complete required cybersecurity modules
- The ISO dashboard showing resolved incidents and trend analytics

- The Admin panel for managing reported threats and generating PDF logs

Each iteration incorporated feedback gathered during class walkthroughs and internal sprint retrospectives.

In the *test* phase, we evaluated the prototype through peer reviews and usability checks. The feedback highlighted the value of the progress bar in the Email Checklist Tool and the importance of visual threat levels (e.g., red dot for urgent). We also validated our layout choices by confirming users could complete key tasks (e.g., reporting an issue) quickly and without confusion.

Overall, this iterative process ensured that our prototype was not only visually clean but also functionally aligned with stakeholder needs and cybersecurity best practices.

III. Independent Learning

This project pushed me to learn independently in areas I wasn't fully confident in at the start — particularly cybersecurity best practices, interface accessibility, and Figma prototyping. Early in the project, I realized that I didn't have a solid grasp of how cybersecurity workflows actually function in a government setting. To address this, I spent time reading the Australian Signals Directorate's Cyber Security Incident Response Planning: Practitioner Guidance (Australian Signals Directorate, 2024). It gave me a clearer understanding of how incident response plans are structured and helped shape the workflows we designed for reporting, classification, and escalation.

I also had to level up my Figma skills. Although I had used it before for UI mockups, I had never worked with things like interactive components, auto layout, or accessibility tagging. I enrolled in a LinkedIn Learning course called *Figma for UX Design* (LinkedIn Learning, 2024), which helped me structure the prototype more professionally. I practiced using reusable components and learned how to make the interface cleaner and more consistent across pages.

Accessibility was another area I hadn't focused on much in past projects. For this one, I knew it was important to make the interface usable for everyone, so I spent time watching YouTube videos and tutorials on accessibility basics. I learned about things like using clear labels, ensuring readable font sizes, and avoiding low-contrast color combinations. I also paid more attention to how layout and spacing can affect readability, especially for users who might not be familiar with digital tools. Most of this learning happened through trial and error while adjusting the Figma prototype.

These efforts definitely made me more confident as a UX designer. I'm leaving this project with a better eye for structure, detail, and accessibility — and a stronger sense of how to research and apply complex design requirements on my own.

IV. Project Management and Team Collaboration

Our team adopted Agile methodologies to manage the scope and progress of the project. We worked in three-week sprints, each beginning with a sprint planning session and concluding with a retrospective. These sprints helped us break down the project into manageable chunks and adjust our goals based on evolving feedback. Agile artifact such as sprint backlogs, were maintained through Jira and discussed during weekly stand-up meetings.

To keep our documentation centralized, we used Confluence extensively. This included documenting persona development, journey maps, decision rationales, and sprint summaries. Each team member was responsible for contributing to Confluence pages to ensure shared understanding and accountability. We also maintained a "project changelog" where we logged major updates and decisions, which was especially helpful when cross-checking sprint goals against actual progress.

I was assigned the role of Product Owner. My responsibilities included translating the client brief into actionable tasks, prioritizing backlog items, and ensuring our prototype aligned with TRADIE's cybersecurity goals. Working closely with our Scrum Master, we facilitated efficient meetings, removed blockers, and helped ensure deliverables were achievable and realistic.

Our workflow was modeled on the Atlassian Team Playbook (Atlassian, 2024), which we adapted to create a team agreement at the beginning of the semester. This agreement detailed availability hours, expectations around asynchronous work (e.g., Discord etiquette), and how we preferred to give and receive feedback. These norms helped foster a respectful and supportive team environment.

Task delegation was based on both individual strengths and learning goals. I led UI design and handled most of the Figma interactions and component structuring. I also organized the visual structure of our Confluence space and kept it up to date with design iterations. Other teammates focused on stakeholder research, report editing, usability testing, and accessibility reviews. We used a Jira Kanban board to visualize our task flow, moving cards across "To Do," "In Progress," "Under Review," and "Done" columns.

Challenges did arise — including one instance where miscommunication around deadlines caused a delay in a deliverable. However, we addressed this transparently during the sprint retrospective and implemented a shared task calendar to improve accountability.

Overall, our collaboration was highly effective because of our consistent communication, shared rituals, and mutual trust. By leaning into Agile principles and using the right tools, we ensured that every member could contribute meaningfully, and we stayed aligned with both client goals and academic outcomes.

V. ACS Code of Professional Conduct

Throughout the TRADIE prototype project, our team adhered to the ethical standards outlined in the Australian Computer Society (ACS) Code of Professional Conduct (Australian Computer Society, 2023). These principles guided our design choices, collaboration, and decision-making to ensure that the final deliverables upheld public interest, professionalism, and quality of life.

A. Public Interest and Privacy

We ensured our design prioritized the public interest by creating accessible and trustworthy tools for reporting cyber incidents. Staff-facing features such as anonymous reporting, plain-language labels, and confirmation screens were implemented to reduce underreporting and build user confidence. We were also mindful of user privacy by avoiding unnecessary data collection and embedding role-based access for sensitive workflows — aligning with the Australian Privacy Act 1988 (Australian Government, 2023).

B. Honesty and Professionalism

All team members committed to giving and receiving feedback constructively. Sprint retrospectives allowed for honest reflection on progress, and decisions were documented transparently in Confluence. As Product Owner, I worked to ensure clarity and realistic scope planning — avoiding overpromising features beyond what the prototype could support. This reinforced professionalism and accountability in client alignment and internal collaboration.

C. Enhancement of Quality of Life

The TRADIE interface was designed to reduce cognitive load and manual effort for users like Alex, the Information Security Officer. By introducing task boards, real-time alerts, and exportable reports, we helped shift the workflow from reactive to proactive. These improvements enhance the well-being of staff and ensure operational efficiency — both key aspects of ethical digital design.

VI. Conclusion

This report has reflected on my individual journey in designing a cybersecurity incident response prototype for TRADIE. Through the application of design thinking, independent learning, collaborative teamwork, and adherence to the ACS Code of Professional Conduct, I have grown both as a UX designer and a responsible digital practitioner.

The project deepened my understanding of human-centered cybersecurity tools and reinforced the importance of empathy, communication, and ethical awareness in systems design. I gained practical experience working with Figma, Jira, and Confluence while contributing meaningfully to a real-world scenario that balanced user needs with regulatory compliance.

Beyond technical skills, this project improved my ability to lead product direction, listen actively to feedback, and uphold transparency in team environments. I leave this experience more confident in both my creative and collaborative capacities, with a stronger foundation in ethical UX practice.

AI Declaration

I declare that this reflection report was written independently. I used AI tools such as ChatGPT to help rephrase, clarify, and improve the tone of certain sections, including grammar suggestions and layout consistency. No content was generated without careful review and revision to ensure originality and personal authenticity. All project-specific reflections, analysis, and experiences are based on my own work. This use of AI complies with Swinburne's academic integrity guidelines.

Appendix

A. Figma Screenshots

Screenshots of key prototype interfaces, including:

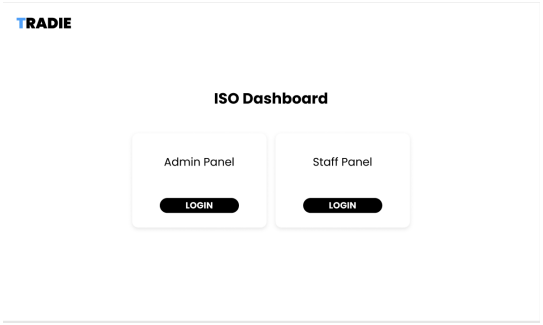

Fig. 1. Iso Incident Dashboard

This page allows the ISO to select between the Admin Panel and Staff Panel. It introduces role-based access control, ensuring that administrative tasks and staff training views are clearly separated and secure.

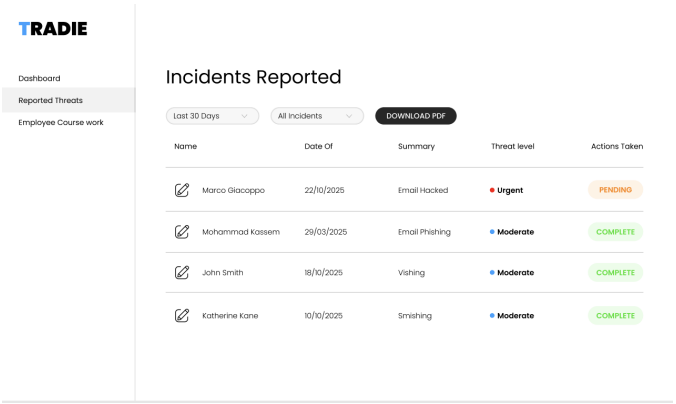

Fig. 2. Reported Threats for Admin Panel

This screen displays the "Incidents Reported" admin panel, where the ISO or administrator can view all reported incidents. The table allows quick filtering by time and threat category, with a "Download PDF" option for exporting logs.

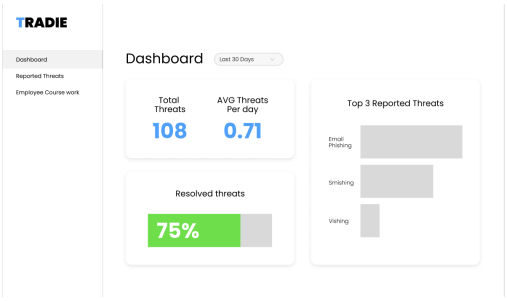

Fig. 3. Dashboard for Admin Panel

The dashboard offers a high-level summary of incident activity over the past 30 days. It displays metrics such as the total number of threats, average threats per day, resolution rate, and top reported incident types.

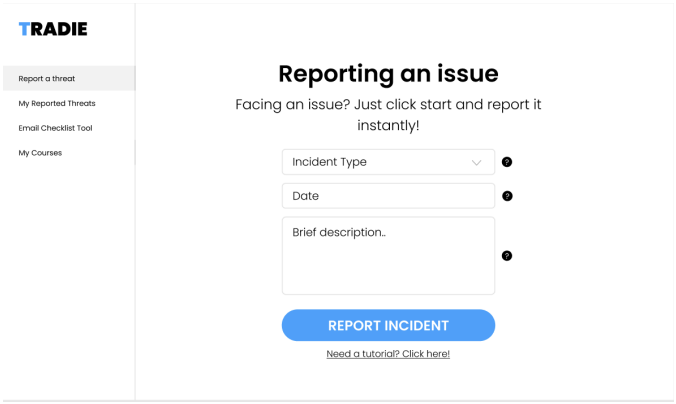

Fig. 4. Incident Report Form

This screen shows the user-friendly form for staff to report cybersecurity incidents. It includes fields for selecting the incident type, date, and a brief description. Helper icons next to each field support users who may be unfamiliar with technical terms, making reporting accessible to all staff.

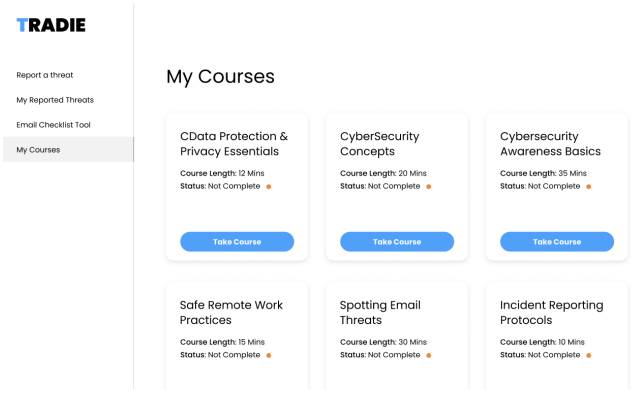

Fig. 5. Staff Training Modules

This interface provides staff with access to cybersecurity training modules. Each course tile displays the title, estimated duration, and completion status, allowing employees to track their progress in building security awareness. It supports TRADIE's goal of ongoing cyber education for all roles.

References

- Atlassian. (2024). *Team Playbook*. https://www.atlassian.com/team-playbook
- Australian Computer Society. (2023). *Code of Professional Ethics*. https://www.acs.org.au/memberships/professional-ethics-conduct-and-complaints.html
- Australian Government. (2023). *Privacy Act 1988*. https://www.legislation.gov.au/Series/C2004A03712
- Australian Signals Directorate. (2022). *Cybersecurity incident response planning: Practitioner guidance*. https://www.cyber.gov.au/resources-business-and-government/governance-and-user-education/incident-response/cybersecurity-incident-response-planning-practitioner-guidance
- Brown, T. (2009). *Change by design: How design thinking creates new alternatives for business and society*. Harvard Business Press.
- LinkedIn Learning. (2024). *Figma for UX design*. https://www.linkedin.com/learning/figma-for-ux-design
- Norman, D. A. (2013). *The design of everyday things* (Revised and expanded edition). Basic Books.