



SHIELD CYBERGAMES

CIC TEAM DIVERSITY

RMIT MELBOURNE

Meet The Team



Jim Moriarty

Bachelor of Business
(Entrepreneurship)



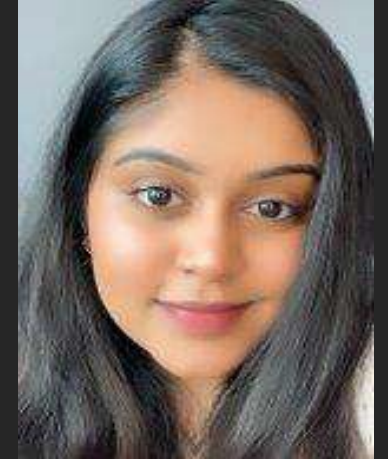
Blake Frost

Bachelor of Engineering
(Aerospace)
Bachelor of Business
(Management)



Gabriel Valentino

Bachelor of Business
(Supply chain &
Logistics)



Raja Cheedhara

Master of Cyber
Security



ResponsibleTech

- **Project:** looks at Tech-Driven Dilemmas in business and aims to analyse the risks and ethical problems associated with the use of technologies in the banking and insurance.
- **Goal:** to create a culturally inclusive and ethically sound workforce globally and to inspire responsible technological innovation.



Who is The Customer?

- Fintech companies & Neo Banks.
- Ransomware costs in 2021 predicted at \$6 trillion.
- 2020 has been one of the worst years for information breaches due to COVID-19.
- Working from home is the main cause.

A close-up, low-key photograph of a person's face, focusing on their eyes and nose. They are wearing dark-rimmed glasses. The lenses of the glasses are reflecting a bright blue light that forms the shape of binary code (0s and 1s). The person's face is partially in shadow, and the overall lighting is dim, with a strong blue tint from the reflection. In the top left corner, there is a small, solid orange horizontal bar.

Problem Statement

- **Original:** “How might we ensure a bank or business response to ransomware is made using ethical principles?”
- **Reframed:** “How might we encourage ethical cybercrime principles, for bank and business employees, so that ransomware attacks are handled responsibly?”



Working Backwards Workshop

- Built many empathy maps to understand our customer
- Used the Crazy8's ideation process
- Tried to understand user experience and customer benefits
- Developed customer testimonials

PRFAQ

VISUALS

Diversity Group with RMIT CIC and AWS Launches Shield CyberGames & ShieldSet

AUSTRALIAN TRIANGULAR REVIEW – 1st November 2021 – Through ransomware attack simulation and guided ethical instruction, [Shield CyberGames & ShieldSet] provides dynamic interaction for NeoDeleka or FinTech to improve cyber awareness and ethical responses to ransomware. Ethical experience with live cyberattacks is now safe through Diversity Group's recently launched [Shield CyberGames & ShieldSet] simulating the process of well-known attacks such as Ransomware, WannaCry, Petya and Bad Rabbit.

In 2020, Accenture reported the average cost of cyber attacks at \$12 million USD, listing banks as enduring the highest average annual cost at \$56.37 million USD. The report stated 75% of companies infected with ransomware have up-to-date endpoint protection and 50% of security professionals state their organisation is not prepared for ransomware attacks. In 2020, 2,800 ransomware attacks were reported to the FBI, and ransom payments totalled \$550 million USD in cryptocurrencies. Furthermore, PwC's estimate by 2021, every 11 seconds a business will fall victim to ransomware, with 40% choosing to pay the ransom. With total costs from ransomware by 2021 at \$6 trillion annually, in response to escalating costs of ransomware and a recent attack by Ransomware criminal network, affecting 200 banks and demanding ransom of \$70 million USD in Bitcoin the Biden Administration has sanctioned dealings with cryptocurrency exchanges which facilitate the payment of ransoms. Frustration among internal security departments and management provides opportunity through initiation of a culture shift promoting the simulation of cyber attacks to educate for ethical cyber awareness. With an estimated 54% increase in ransomware in the first half of 2021 when compared to the first half of 2020, cyber awareness has never been more necessary.

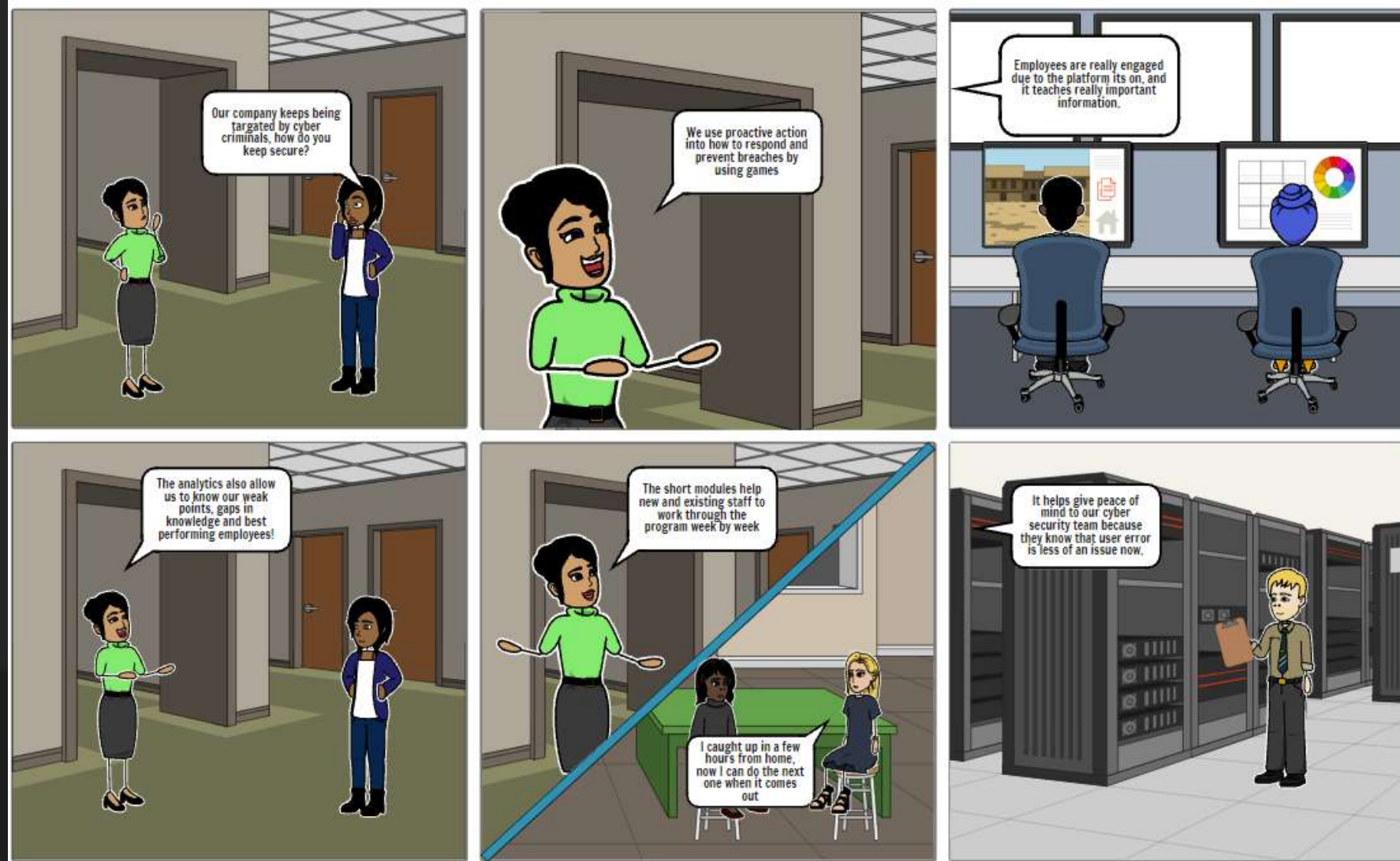
[Shield CyberGames & ShieldSet] are designed for users of all levels of cybersecurity knowledge. Through the simulated cyberattacks, users learn proactive ethical cybersecurity measures. Diversity Group aims to provide this value through experiential and adaptive learning. The cyberattack simulations in [Shield CyberGames & ShieldSet] will provide proactive knowledge for all NeoDeleka and FinTech employees, ensuring organisations are cyber-ready, enhancing problem-solving skills when dealing with breaches, and build confidence. The games are designed to test the user for existing knowledge and place the user into the attack simulation which tests their existing skills. At the end of the game the user is directed to the appropriate learning module designed to advance the user's skillset. Scoring of ethical responsibility awareness and simulation responses are available for the security executives to track employee performance.

Continuously updated ransomware attack simulations deliver experience with real-world cyber security issues. Moreover, [Shield CyberGames & ShieldSet] guide the player through being attacked, allowing the player to gain genuine experience from a safe cyber environment. Playing a responsive role of defender, players are guided through ingenuity to deal with the attacks. [Shield CyberGames] are a subscription service offering ethical simulation of ransomware. [ShieldSet] includes the games with advanced training modules tailored using game results.

Prime Minister Boris Johnson's office has released a statement which further reinforces the importance of cyber security: "the National security strategy" which will set out the importance of cyber technology to our way of life – whether it's defeating our enemies on the battlefield, making the Internet a safer place or developing cutting-edge tech to improve people's lives."

Kelley – FinTech CIO – "Training my staff in the importance of cyber hygiene and ethics has never been easier. Now with the [Shield CyberGames & ShieldSet] from Diversity Group, I have a way of measuring my staff's awareness levels. I can direct the staff to the proper training they need, and I can reward those staff members who are always ethical and respond well with incentives. The games are fun and interactive. With regular updates which draw parallels to real-world attacks, my staff can live in the hot seat of a real attack from the safety of a simulated environment."

Call To Action – <https://www.shieldcybergames.com/subscribe>



A dark, high-contrast background image featuring various gaming peripherals. In the upper right, there is a black game controller with a glowing blue directional pad and a black mouse with blue light bars. Below the controller, a black keyboard is partially visible. In the lower right, a red and black braided cable is coiled. The overall aesthetic is sleek and modern, typical of gaming hardware marketing.

The Idea: Shield CyberGames & ShieldSet

- Based on real-life situation and user-response
- Firsthand victim perspective
- Set modules teach users about cyber-attacks, preventive measures, and response techniques



Why Do We Need It?

- Maintain company reputation and customer's trust
- Protect company's valuable assets from loss

A photograph of two hikers on a rocky mountain peak. One hiker, wearing a yellow jacket and a white helmet, is standing and reaching out to help another hiker, who is wearing a red jacket and a red beanie, climb up. The background shows a cloudy sky. The image is partially obscured by a dark, semi-transparent overlay on the right side, which contains the text.

How Does Shield CyberGames Help?

- Reduce cyber-attacks risks, increase cyber-security knowledge and skills for users of all levels
- Practice instant and ethical respond to ransomware through all-in-one guides

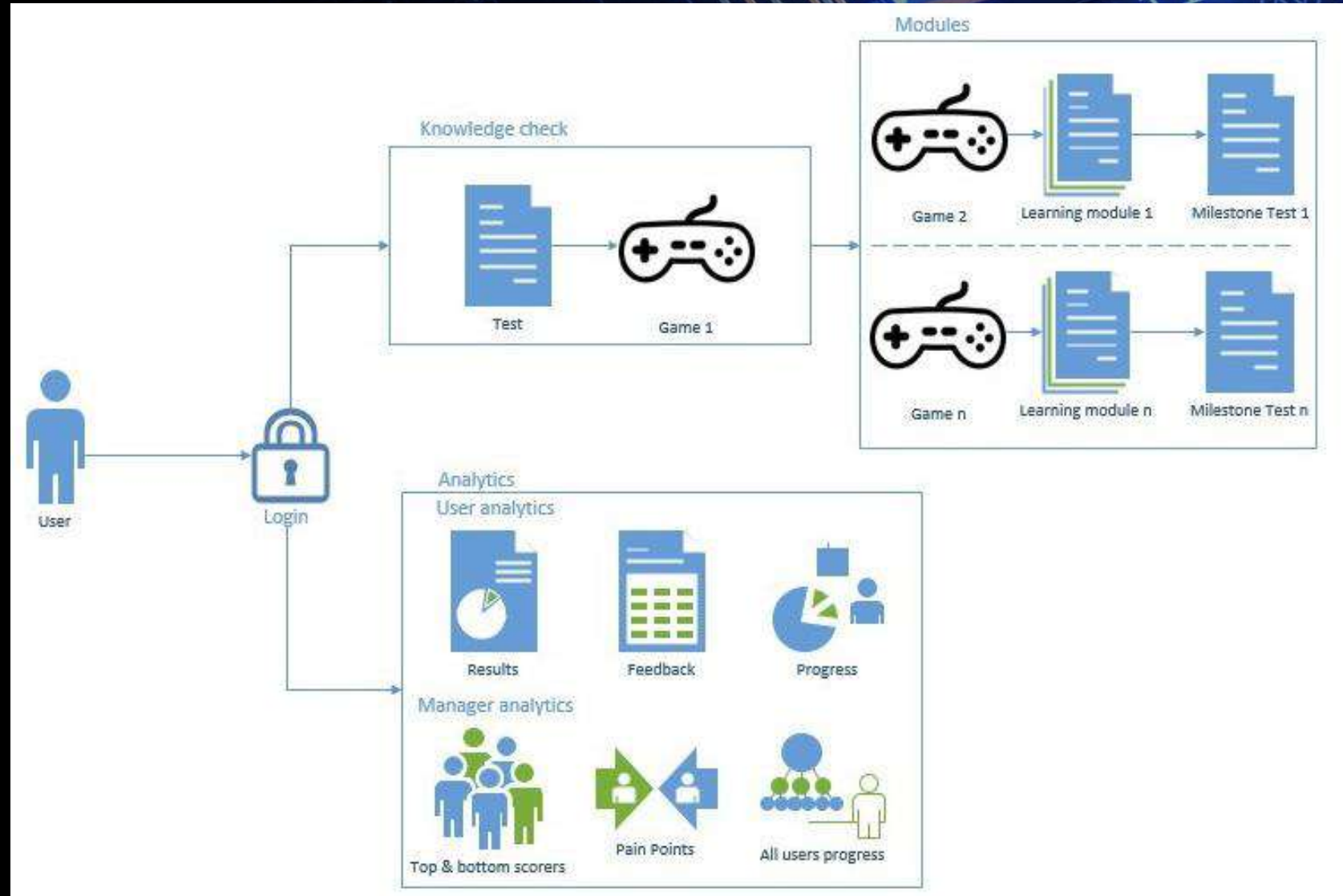
The background of the slide is a photograph of a person's hand using a black pen to draw wireframe diagrams on a large sheet of white paper. The wireframes consist of various rectangular boxes and connecting lines, representing a user interface layout. A yellow and black spirit level is placed horizontally across the middle of the paper. In the bottom right corner, a portion of a black calculator is visible. The left side of the image is overlaid with a dark, semi-transparent gradient.

Prototyping

Steps - Services - Wireframes

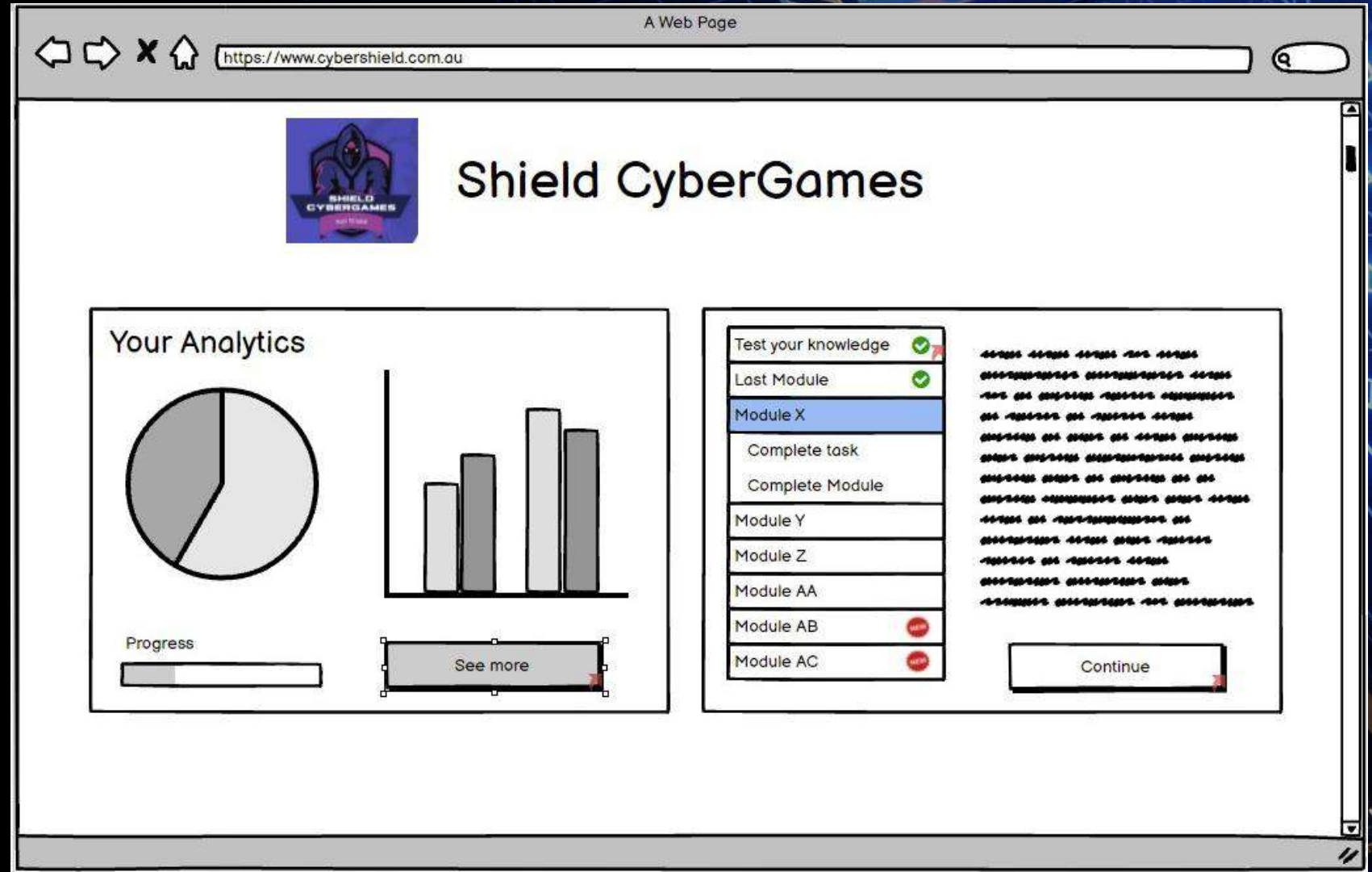
Design Architecture Representation

- Login through organisation e-mail ID
- User analytics: results, progress, and feedback.
- Manager analytics: Top and bottom scorers, pain-points and overall progress.
- Learning and gaming room: knowledge check, modules, games.
- Adaptive learning approach.



Landing Page

- The users have two options: Analytics or Learning and gaming progress.



Knowledge Check

- Entry-level questions to check the users' knowledge about cybercrimes.
- Adaptive learning: This will decide the type and difficulty levels of the questions that follow.

A Web Page
https://www.cybershield.com.au

KNOWLEDGE CHECK

1. How much would you say you know about Cyber Security? ?

- ☒ A lot
- ☐ Quite a lot
- ☐ Some
- ☐ None

2. What is the leading cause of Cyber Breaches? ?

- ☐ Brute force
- ☒ Targetted hacking
- ☐ Phishing emails
- ☐ Human error

Knowing the most common causes of cyber breaches will help to be more cautious around these area, knowing where your best security measures must be.

3. Your company is the victim of a ransomware attack, which responses are most ethical? ?

- ☐ Pay the ransom
- ☒ Ignore the requests
- ☐ Contact ASIC
- ☒ Keep it hidden
- ☒ Close the company

Submit

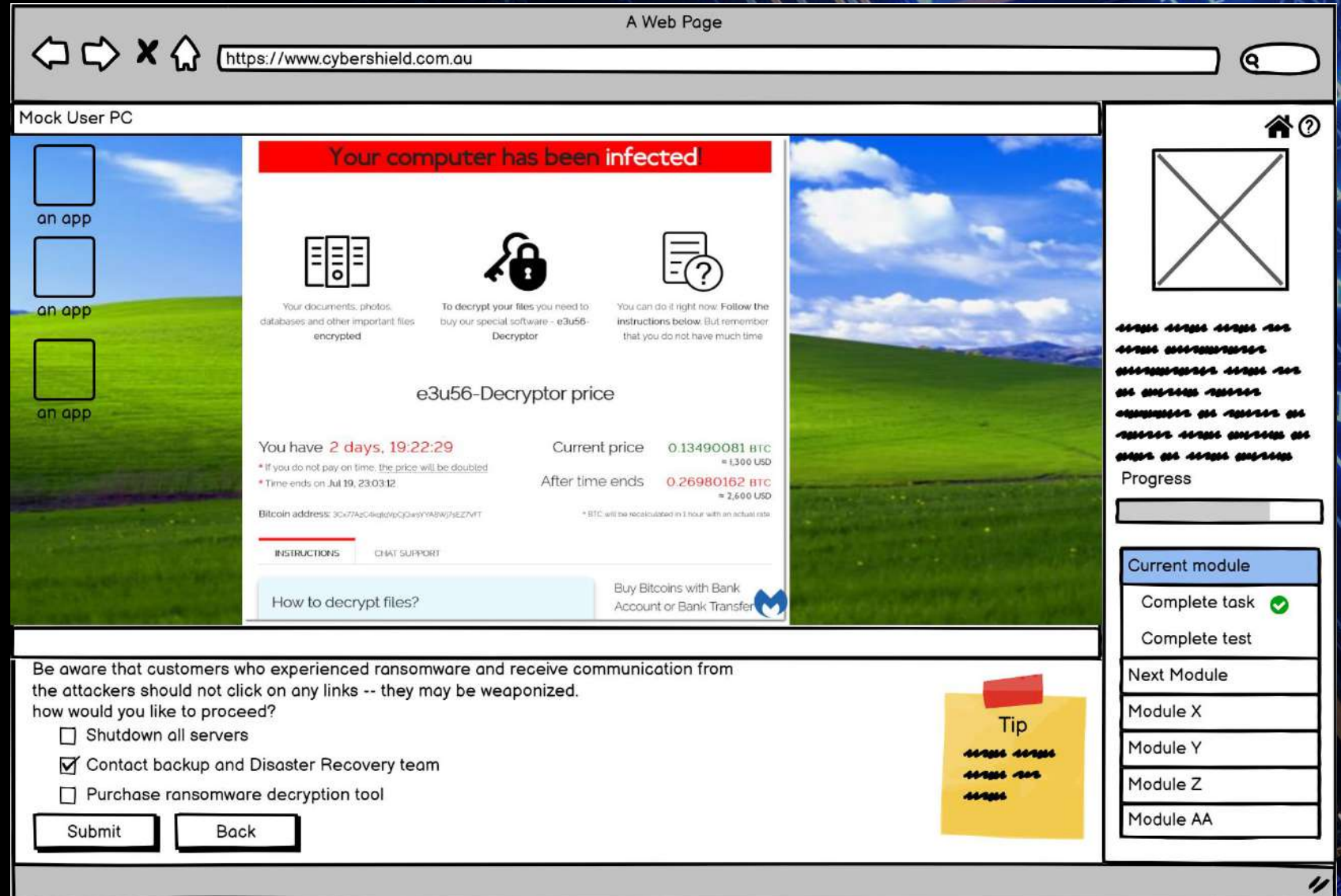
Progress

Test your knowledge

- Knowledge check
- Quick Game
- Next Module
- Module X
- Module Y
- Module Z
- Module AA

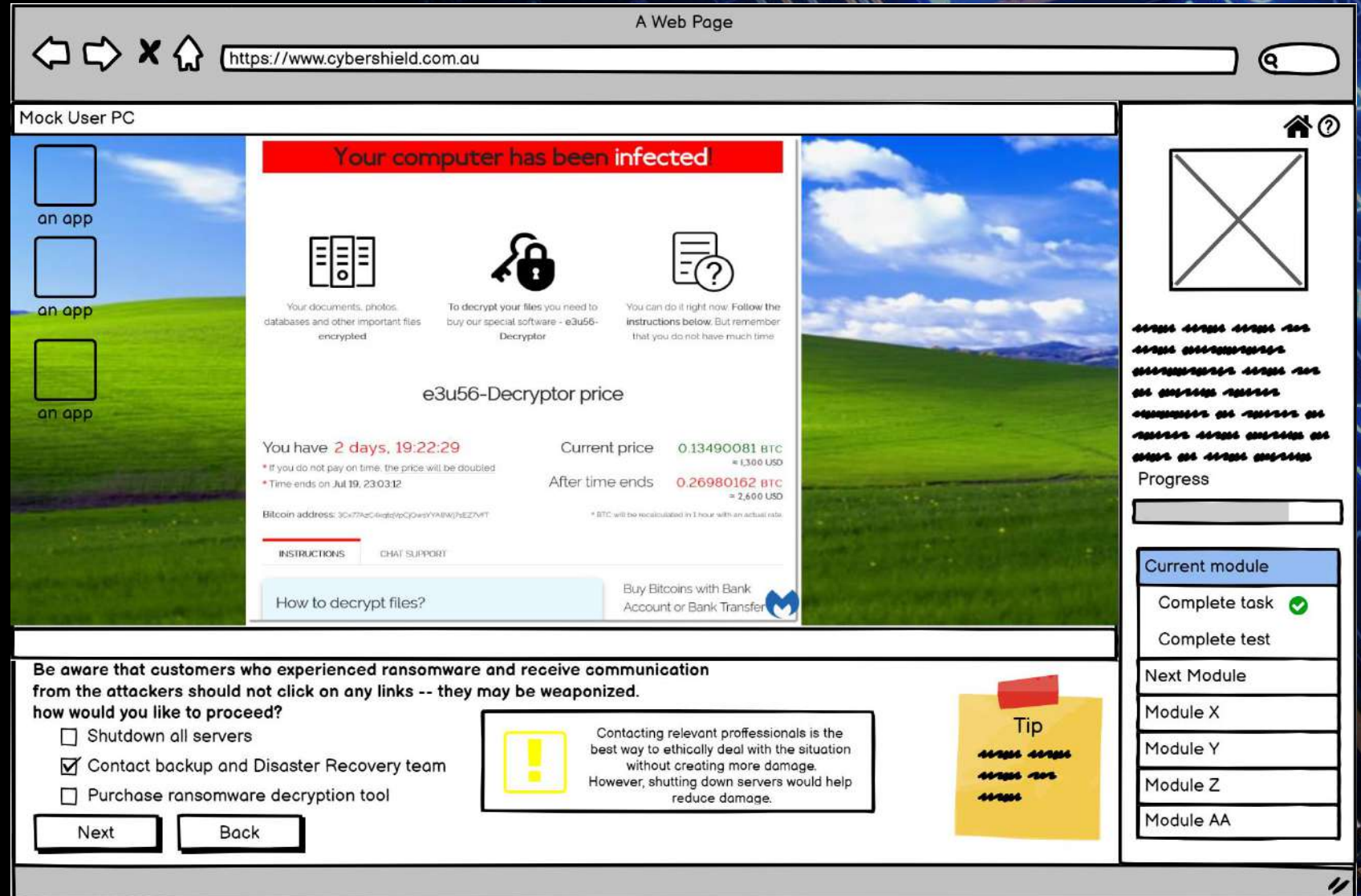
In Game

- The gaming screen has tips and progress details.
- It also has a ransomware attack warning that's inserted based on the Revil ransomware attack.
- The question here is based off the timeline of the Revil attack.



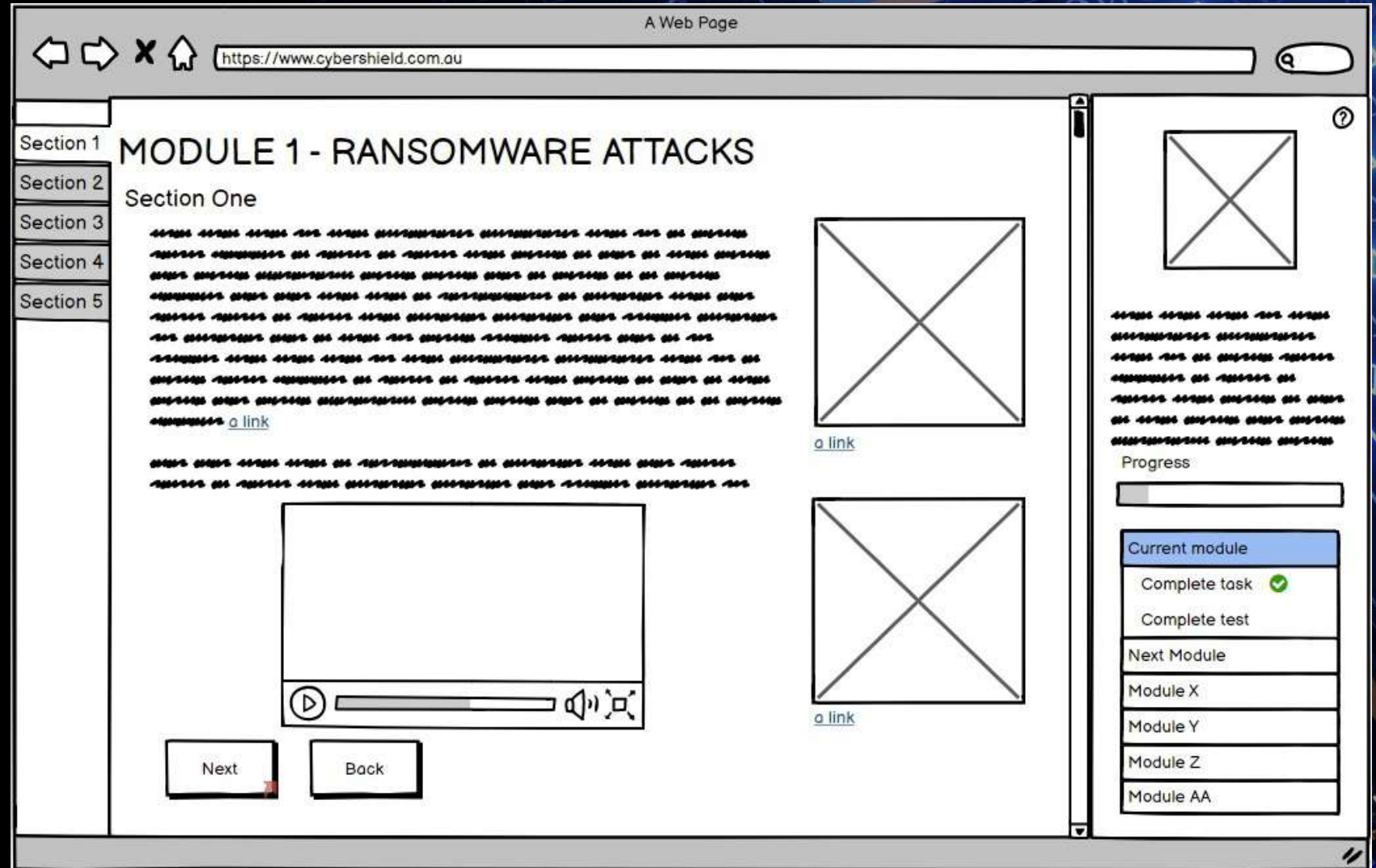
In Game

- The user will be supplied with error messages.
- The feedback will be open ended, meaning that there will be an explanation for the input along with displaying whether it is correct, incorrect or partially correct.



Learning Modules

- Different section will cover different topics under the module
- Interactive and fast paced learning modules are key to focus
- Adaptive from the game, some section may be skipped, and others put more focus on.



Example Test

- Based on game and module learnings
- Tests will be one question at a time with instant feedback
- May vary from short to scenario questions
- All multiple choice, but not always just one answer

A Web Page

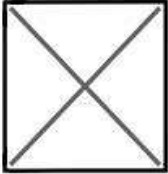
https://www.cybershield.com.au

MODULE 1 - RANSOMWARE ATTACKS

MODULE TEST


1. Select all ways you can reduce damage from a ransomware attack

- ☐ Segment user data
- ☐ Reduce forward facing data
- ☒ Change your password often
- ☐ Update your OS as soon as it's available



Progress

Current module

Complete task 

Complete test

Next Module

Module X

Module Y

Module Z

Module AA

Example Test

- Feedback will be detailed and instant
- Failing score of 70 to ensure the knowledge is learnt
- Question pool so that the module may be repeated if needed
- Each module will take about an hour including the game

A Web Page


https://www.cybershield.com.au

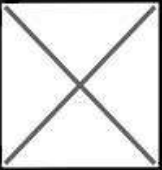
MODULE 1 - RANSOMWARE ATTACKS

MODULE TEST

1. Select all ways you can reduce damage from a ransomware attack


- ☐ Segment user data
- ☐ Reduce forward facing data
- ☒ Change your password often
- ☐ Update your OS as soon as it's available

 Changing your password will increase the overall security of your system, however it will not aid in the reduction of damage given a ransomware attack



Progress

Current module

Complete task 

Complete test

Next Module

Module X

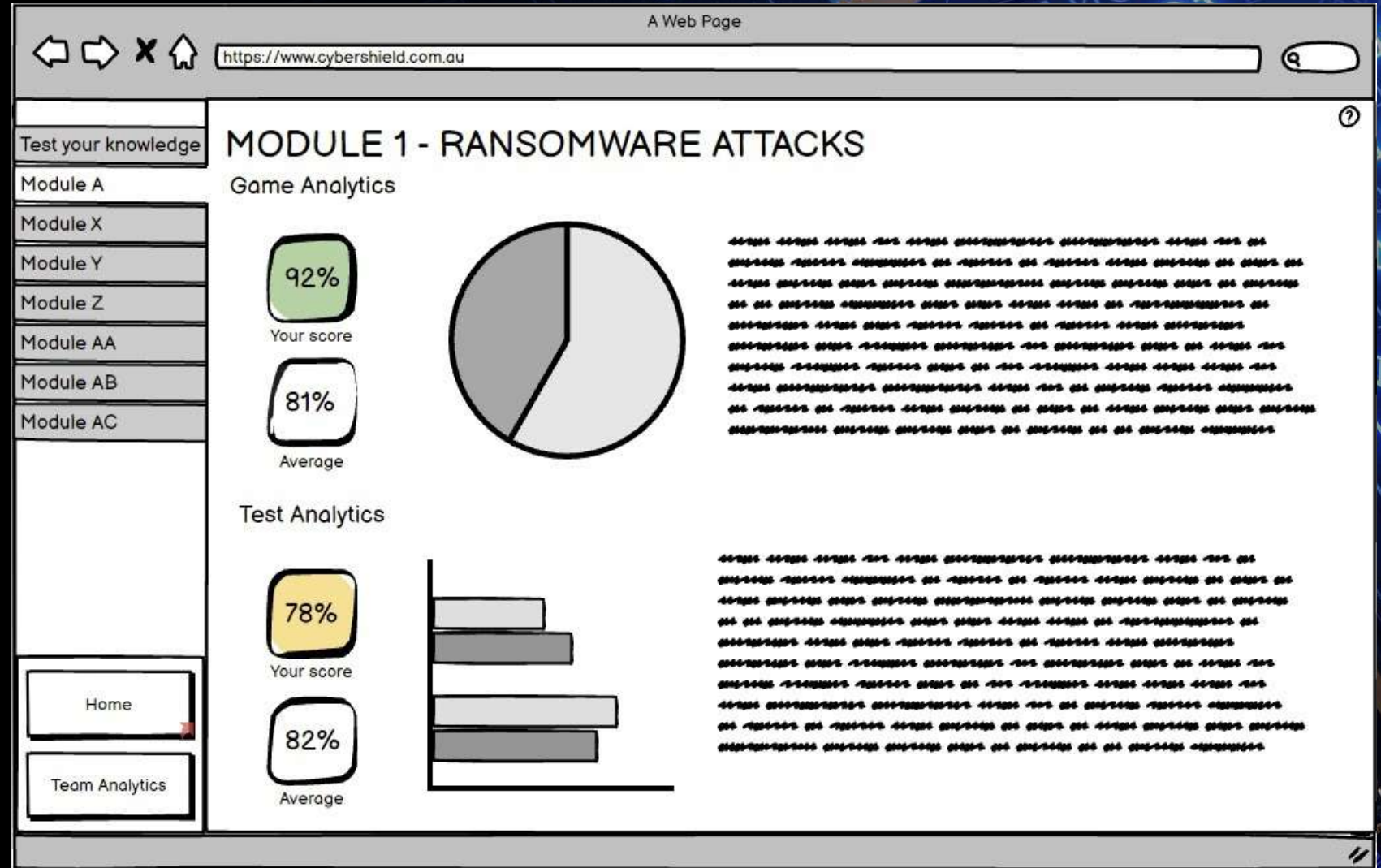
Module Y

Module Z

Module AA

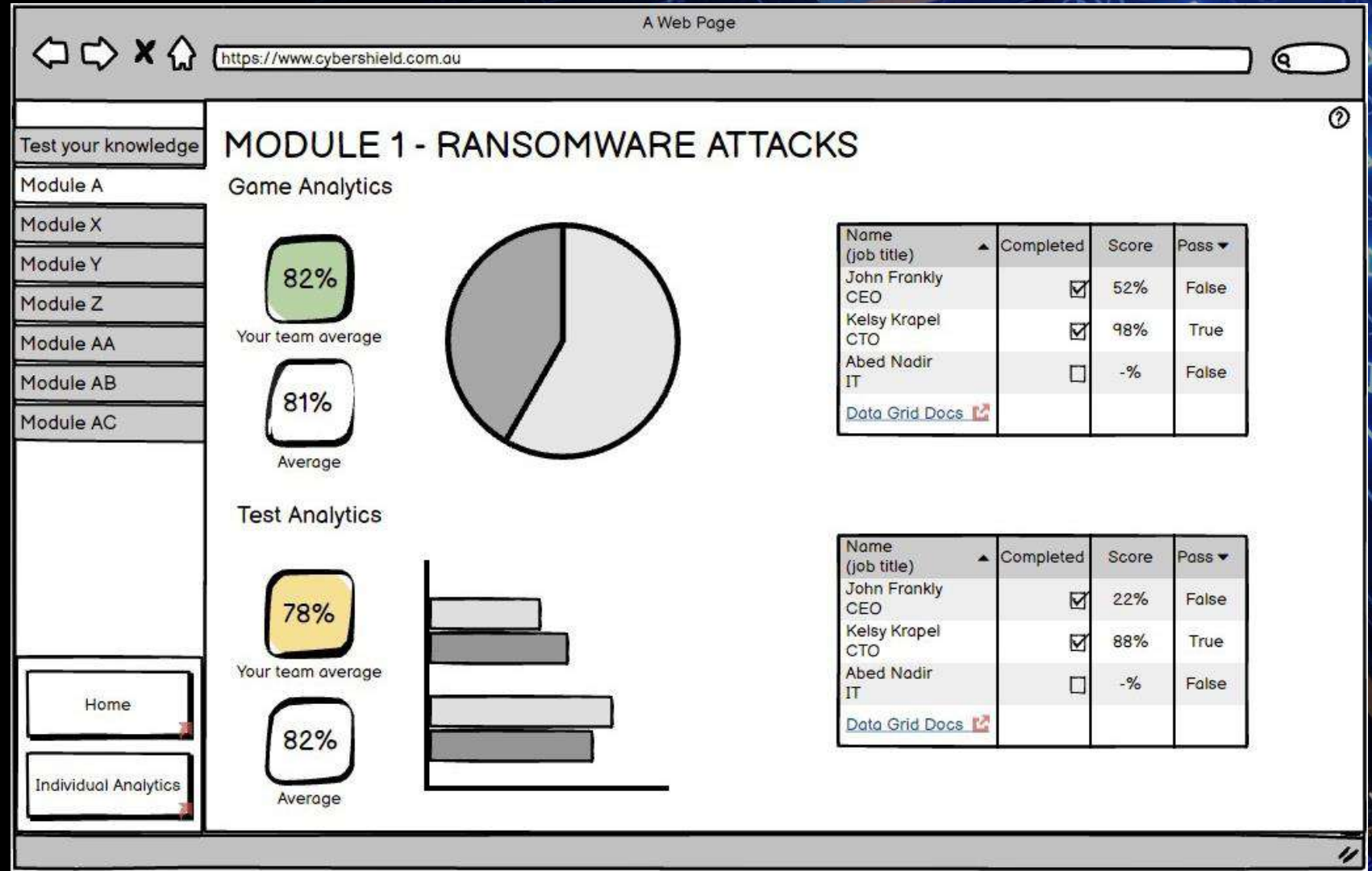
Game Analytics

- Individual analytics will show how the user scored compared to the pack
- Provides detailed feedback about the pain points in both the game and test



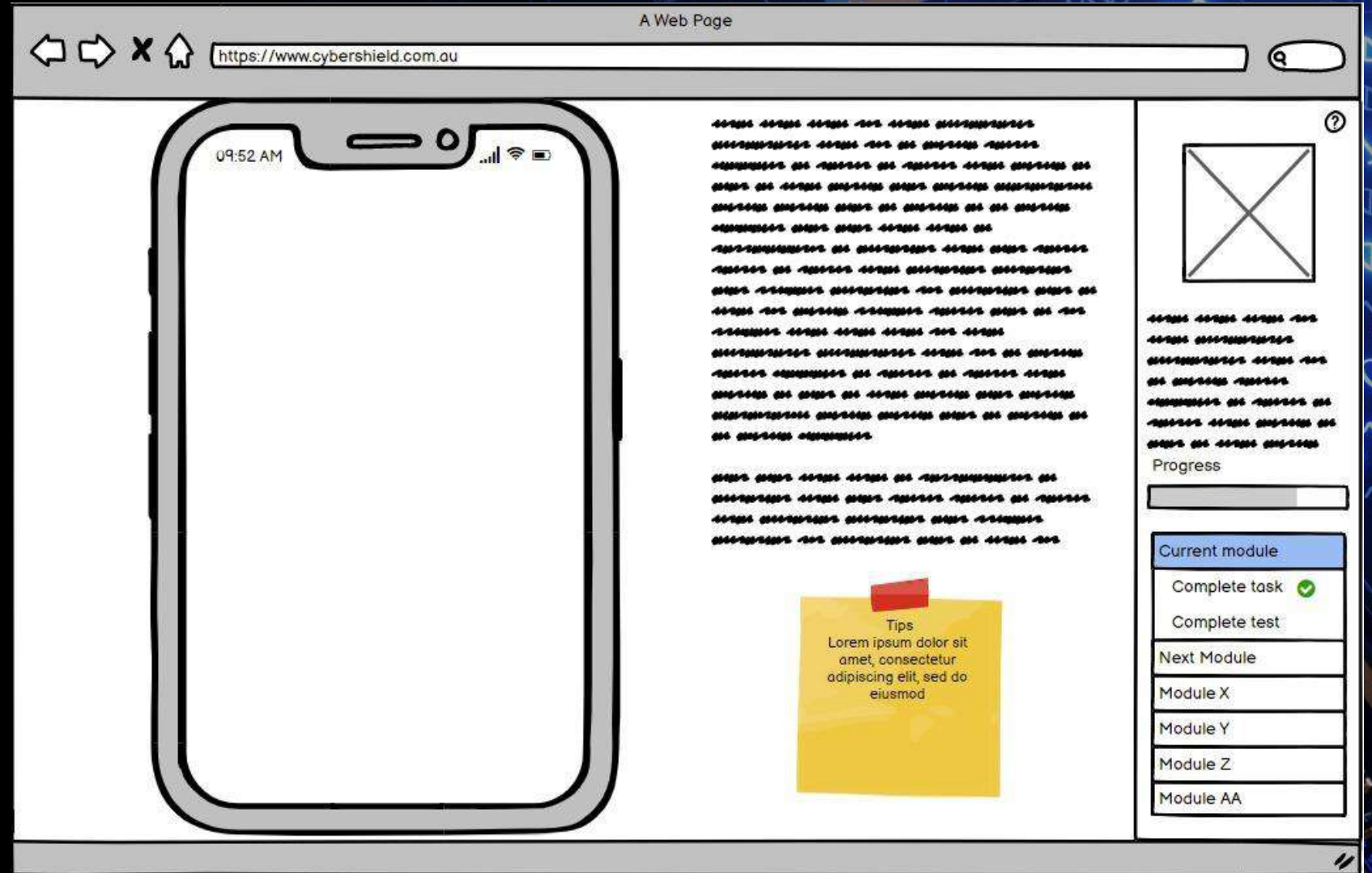
Game Analytics

- Manager analytics will show the total teams average compared to other teams
- Tracks progress and scores for each module to identify pain points
- Lower scoring users or users who fall behind can be supported more by the cyber security team



Future Development

- More modules will be added on an ongoing basis to stay up to date
- Subscription service will be more fleshed out
- Mobile integration will increase accessibility





Thank you!

- Centre for Human Rights and International Justice at Stanford University
- AWS
- RMIT CIC
- Bobbie Couhbor
- Catherine Eibner
- Eskil Olav Andersen
- Geetika Verma
- Georgia Smith
- Joanne Hall
- Julian Waters-Lynch
- Keith Archibald
- Matt Salier
- Meg San Miguel
- Nivetha Thandapani
- Søren Juul Jørgensen
- Zian Fernandes



Q&A