🟦 Slide 1: Title Slide — *Speaker 1*

Script:

"Good day, everyone. We are here to present our literature review on *Cybersecurity Threats and Awareness in Higher Education*. As technology continues to transform education, it also brings a growing list of cybersecurity risks. These risks are not only technical but also behavioral and institutional.

🟦 Slide 2: Introduction — *Speaker 1*

Script:

"In recent years, higher education institutions have become major targets for cyberattacks. These institutions store large volumes of sensitive data—from research outputs to student records—and often lack the advanced cybersecurity infrastructure used by corporate or government entities.

In the Philippines, this problem is intensified. Many universities and colleges operate on outdated systems with limited IT staff and low budgets for digital security. This makes them attractive and easy targets.

This review aims to:

1. Identify and describe the major cybersecurity threats faced by higher education institutions, and

2. Explore how awareness of these threats varies across different demographic groups within the academic community.

Let's first examine the threats themselves."

🟦 Slide 3: Thematic Review – Common Threats — *Speaker 1*

Script:

"Cyber threats in higher education can be categorized into external and internal types. External threats include ransomware, phishing attacks, spyware, trojans, and Distributed Denial of Service (DDoS) attacks. These can paralyze networks,

compromise data, or demand financial ransom.
For example, in 2023, 79% of higher education institutions globally were hit by ransomware attacks according to Sophos. That's an alarming number—one that shows just how vulnerable this sector is. But external threats are only half the story. Internal threats—such as human error, lack of awareness, and insider misuse—are equally, if not more, dangerous. For example a staff member clicking a phishing link, or a student downloading infected software, can open the door to a breach just as easily as an outside hacker."

🟦 Slide 5: Theme 2 – Demographic Variations in Awareness — *Speaker 1*

Script:

"Now that we've seen the kinds of threats institutions face, let's look at how well people within these institutions understand those risks.
Cybersecurity awareness is not evenly distributed. According to the literature, awareness tends to vary significantly by **role**, **age**, and **gender**.
Administrative staff usually have higher levels of awareness. This may be because they deal with confidential records and are often included in security briefings. In contrast, **students**, especially **younger undergraduates**, are the least aware. Many of them have grown up in a digital world but lack training in recognizing threats.
Gender-based studies also reveal differences—though findings vary, some suggest that males may be more confident in their cybersecurity skills, while females may be more cautious.
These insights make it clear: a one-size-fits-all approach to cybersecurity education simply doesn't work. Training needs to be **customized** to different user groups."

🟦 Slide 6: Chronological Trends (2020–2024) — *Speaker 2*

Script:

"Another important theme is how research itself has evolved over time. From 2020 to 2021, the focus of most studies was on technological solutions—anti-virus software, firewalls, and system hardening.

But from 2022 to 2024, the lens began to shift. Researchers started to pay closer attention to **human behavior**, **cultural norms**, and **individual decision-making**.

For instance, some studies explored how culture influences one's perception of risk or how users interpret warning messages.

However, there's a major gap in the research: very few **longitudinal studies** track how cybersecurity behavior changes over time. We need more long-term research to understand what types of training and policies actually lead to sustained behavioral change."

🟦 Slide 7: Research Methods — *Speaker 2*

Script:

"To investigate these themes, researchers have used a variety of methodologies.

- **Quantitative surveys** are commonly used to measure awareness levels across large populations.

- **Qualitative case studies** offer deeper, contextual insights, often conducted within specific institutions.

- **Mixed methods** studies combine the two, offering both statistical trends and narrative depth.

  But there's a consistent issue: most of the data is **self-reported**. This introduces bias—people may overestimate their knowledge or underreport risky behaviors.

  This limitation highlights the need for more objective, behavior-based evaluations in future research.

Slide 8: Synthesis – Presenter 3

To sum up what we have learned from this review, cybersecurity threats in higher education are becoming more serious and harder to manage. Threats like ransomware, phishing, malware, and insider attacks are now very common in universities.

Here in the Philippines, the situation is even more challenging. Many schools use outdated systems, have weak security policies, and don’t have enough funding or trained IT staff. These issues make schools easier targets for attackers.

Another key finding is the gap between what people know and what they actually do. For example, someone might understand what a phishing email looks like, but still click on it out of habit or carelessness.

This shows us that cybersecurity isn’t just about giving information—it’s about changing behavior. People need to develop good habits and feel responsible for protecting their digital space, especially in an academic setting."

Slide 9: Conclusion – Presenter 3

"In conclusion, we face serious but solvable challenges.

Cyberattacks are increasing in both number and complexity, and higher education is a clear target. Philippine universities are especially at risk because of weak systems and limited resources.

We also saw that different groups like staff, faculty, and students have different levels of awareness. Students, especially the younger ones, are often the least aware and the most at risk.

And most importantly, just knowing about cybersecurity isn’t enough. We need training that helps people change their online habits. This means making programs that are suited to different roles and age groups.

To truly improve cybersecurity, future research needs to focus more on Southeast Asia, study behavior over time, and help shape better school policies. That way, we can go beyond reacting to threats and start preventing them."

Slide 10: Thank You – Presenter 3

"Thank you so much for listening to our presentation. If you have any questions, please don’t wag pls. Okay na toh~~~"