* Title: Embedding Human-Centric Cybersecurity in Start-Up Environments
* Presenter: Milad Chowdhury
* Date: 18/04/2025

**Slides 1 & 2– Introduction**

Hello and welcome, my name is Milad Chowdhury, and today I’ll be presenting on embedding human-centric cybersecurity in start-up environments - Solutions to Human Factors and Ethical Challenges. I’ll discuss practical and ethical ways to strengthen cybersecurity in the start-up. This builds on my earlier assessment, where I explored how human factors like social engineering, insider threats, and weak security culture can create major risks. In the next ten minutes, I’ll share solutions combining behaviour-focused techniques, technical controls, and ethical principles. We’ll also explore how emerging technologies, like generative AI, change how organisations think about security.

**Slide 3 – Understanding Human-Centric Cybersecurity**

Human-centric cybersecurity is based on the understanding that technology alone is not enough. People, their behaviours, and their values shape an organisation’s ability to remain secure. In start-ups, limited resources and rapid development cycles mean employees often take on multiple roles. This can result in shortcuts, workarounds, and reduced vigilance. A human-centric approach combines awareness, usability, and responsibility to foster an environment where secure practices are intuitive, supported, and reinforced by leadership.

**Slide 3 – Behavioural + Technical Integration**

So, how do we combine behaviour and technology? A great place to start is with mental models. According to Wash (2010), people build mental shortcuts to understand threats, and these models affect how they respond. If training and tools align with users' thinking, they’ll be more effective. So, we should use realistic scenarios and clear prompts alongside things like multi-factor authentication and access controls.

**Slide 4 – Tackling Social Engineering**

Social engineering, especially phishing, is one of the most common ways attackers get in. Start-ups can use phishing simulations to help people recognise suspicious emails and learn how to respond. These exercises can make a big difference when paired with feedback, short videos, or guided walkthroughs. But it’s important to make training feel supportive, not stressful. No one wants to feel tricked or humiliated.

**Slide 5 – Ethical Training Design**

That brings us to ethics. According to the Menlo Report, training must respect individuals' dignity and autonomy. This means employees should know why training is happening, what data is collected, and how it will be used. Using punishments or public scoreboards can harm morale. Instead, training should build confidence and help staff feel part of the solution, not the problem.

**Slide 6 – Insider Threats in Start-Ups**

Insider threats are another issue, especially in start-ups where people wear many hats and might have broad system access. The NIST SP 800-53 framework recommends using least privilege principles—people only get access to what they need. In addition, research from Greitzer and Frincke (2010) shows that stress, isolation, or job dissatisfaction can be early signs of risk. So, it’s about supporting employees, not just monitoring them.

**Slide 7 – Surveillance vs. Trust**

Speaking of monitoring, it’s a sensitive topic. Reeves et al. (2021) argue that too much surveillance can backfire, leading to fatigue, disengagement, or resentment. The solution is transparency. Explain what’s being monitored and why. Offer opt-in tools when possible. Let people know it’s about keeping everyone safe, not watching their every move.

**Slide 8 – Building a Security-First Culture**

A strong security culture doesn’t happen overnight. It has to be built into daily habits, team norms, and leadership behaviour. Schlienger and Teufel (2003) emphasise the role of leadership in setting the tone. If managers take security seriously, employees are more likely to follow. Start-ups can use gamified training, real-life scenarios, and rewards to make security engaging and relevant.

**Slide 9 – Inclusive and Equitable Training**

We also need to ensure that training is inclusive. The Menlo Report’s Justice principle reminds us that one-size-fits-all doesn’t work. People learn in different ways. Some need more time, while others benefit from visual tools or hands-on practice. We must ensure everyone has a fair chance to understand and apply security practices. It’s not just ethical—it also strengthens the organisation.

**Slide 10 – Generative AI: New Frontiers of Risk**

Generative AI brings new risks—deepfakes, fake emails, and AI-driven scams are more challenging to detect than ever. Start-ups must train teams to spot and report these threats using real-world examples and simulations. The NIST AI Risk Management Framework (2023) advises that AI tools should be transparent, fair, and always monitored by humans. Security decisions should never rely solely on algorithms.

AI can be powerful, but without control and awareness, it can become a threat. Combining human judgment with policy and training is key to staying secure.

**Slide 11 – Final Thoughts**

To wrap up, cybersecurity isn’t just a technical issue, it’s a human one. The risks are real in start-ups, but the opportunities to get it right are even more significant. By applying behavioural models, using ethical principles, and preparing for future risks like AI, organisations can build systems that are not only secure but also trusted and inclusive. A human-centric approach empowers teams, supports resilience, and embeds security into the organisation's culture.

Leaders play a key role in modelling secure behaviours and setting expectations. Training must be continuous, inclusive, and relevant to the real threats people face. Ethical design and transparency must guide every decision, from policy to platform. When people feel respected, prepared, and involved, they become the strongest defence in any organisation.

This is the end of my presentation. Thank you very much for listening.

**Word Counts:**

* Transcript (spoken script): 880 words
* Presentation slides (titles + bullet points): 335 words
* Combined Total Word Counts: 1215 words