Abstract – This document serves as an analysis of role women play in the field of cybersecurity, discovering their contributions across various industries while subtly pointing out how they've been carrying the load all along. The analysis dives into several key aspects, including the historical context and examining technologies developed or significantly influenced by women, emphasizing their technological advancements that have kept the industry from falling into the dark ages. The analysis further explores the influence of women in cybersecurity across various sectors such as smart cities, railways, maritime, pharmaceutical/biotech, and cyberbiosecurity, demonstrating their undeniable impact on these industries.

This document provides a qualitative synthesis of various aspects, offering valuable insights for security professionals and specialists across different industries. By understanding the unique contributions and perspectives of women in cybersecurity, stakeholders can finally start to appreciate the importance of diversity in enhancing security measures and driving innovation. This analysis is not just beneficial but essential for developing more inclusive cybersecurity strategies, improving industry practices, and inspiring the next generation of cybersecurity professionals.

I. INTRODUCTION

In perpetually evolving world of cybersecurity, women have finally stepped up to show everyone how it's done. Historically underrepresented, women are now making their mark, with projections suggesting they'll make up 30 percent of the global cybersecurity workforce by 2025 and 35 percent by 2031. This increase in representation is a key to unlocking innovative solutions and growth in the cybersecurity sector.

Women in cybersecurity bring a treasure trove of expertise, resilience, and innovation to the table, tackling the complex task of securing a digital landscape with a finesse that’s been sorely missing. Their contributions span various domains, from developing secure smart city technologies to bolstering the cybersecurity of critical infrastructure sectors like railways and maritime. They are also pushing for more inclusive and diverse work environments, which, surprise, are crucial for fostering creativity and comprehensive problem-solving.

A. Women Pioneering Innovation in Cybersecurity

Michelle Drolet, as the Founder and CEO of Towerwall,, she's been a game-changer in shaping information security practices and raising awareness with her expert insights. Keren Elazari is the ethical hacker and researcher who’s not only emphasizing the importance of ethical hacking but also inspiring the next generation of cybersecurity professionals with her captivating talks and research. Mei Leng Tham is the Ministry Chief Information Security Officer at the Ministry of Sustainability and the Environment in Singapore, who’s leading cybersecurity initiatives across various agencies and helping them develop robust cyber and data security strategies.

The contributions of women in cybersecurity aren't confined to leadership roles. They're also at the forefront of developing groundbreaking technologies and methodologies. For example, Avivit Kotler, CISO and DPO at Clalit Health Services, is an expert in risk management and business continuity, ensuring the security of sensitive health data. And Sam King, CEO of Veracode, has significantly advanced application security, making it a critical component of modern security practices.

Of course, despite all this progress, challenges remain. Gender biases and stereotypes still plague the field, often steering women away from pursuing careers in cybersecurity. However, initiatives aimed at promoting diversity and inclusion, such as mentorship programs and educational opportunities, are helping to bridge this gap. Organizations are increasingly recognizing the value of diverse teams in identifying and addressing cybersecurity risks more effectively.

B. Motivation

Let's face it: the motivation behind this analysis is to finally give credit where credit is due. Diversity and inclusion aren't just buzzwords; they're the secret sauce to effective cybersecurity. As our digital world gets more tangled and complex, the need for fresh perspectives and innovative solutions is more urgent than ever. By shining a spotlight on the contributions of women in cybersecurity, this analysis aims to:

- **Promote Diversity**: Let's advocate for more gender diversity in the cybersecurity workforce. Diverse teams aren't just nice-to-have; they're essential for effective problem-solving and can anticipate and mitigate a wider range of threats than the usual homogenous groups.
- **Inspire Future Generations**: We need to provide role models for young women and girls considering careers in cybersecurity. By highlighting the achievements of women in the field, we can inspire the next generation to step up and show the world how it's done.
- **Address Gender Biases**: It's time to call out and dismantle the gender biases and stereotypes that still plague the industry. Understanding these barriers is the first step toward creating a more inclusive and supportive environment for all security professionals.
- **Enhance Industry Practices**: Offer valuable insights that can help organizations develop more inclusive cybersecurity strategies and improve industry practices and finally move past their outdated methods and embrace a more effective approach to cybersecurity.

II. WOMEN CYBERSECURITY LANDSCAPE

A. State of underrepresentation

1) Maritime Industry

- Women are significantly underrepresented in the maritime workforce, including in cybersecurity roles. Only around 2% of the world's 2 million seafarers are women.
- Efforts are underway to increase gender diversity, such as the IMO's annual International Day for Women in Maritime to raise awareness and the Pacific Community's Regional Strategy for Pacific Women in Maritime.
- Challenges include lack of gender-sensitive policies, discrimination, and lack of proper safety equipment/facilities for women on ships.
- Organizations like the Women's International Shipping & Trading Association (WISTA) are working to support and promote women in maritime, including cybersecurity roles.

2) Smart Cities

- Women play crucial roles in developing smart city technologies, including cybersecurity. Anjana Rajan is a human rights technologist working on secure smart city solutions.
- However, the tech industry in general still faces a significant gender gap. Efforts are needed to encourage more women into STEM fields that feed into smart city development.
- Cybersecurity is vital for smart cities which integrate many interconnected systems, so having diverse perspectives from women cybersecurity experts is valuable.

3) Railways

- The rail industry has traditionally been male-dominated, but women are increasingly entering the field, including in cybersecurity roles focused on areas like rail cybersecurity.
- UNIFE, the European Rail Supply Industry Association, has a Gender Equity Advisory Group promoting gender diversity and highlighting the opportunities for women in rail.

4) Pharmaceutical/Biotech

- The broader STEM fields involving these industries face similar gender gaps.
- Encouraging girls' participation in STEM education from an early age is crucial to increasing female representation in cybersecurity across all technology-driven industries.
- Having women cybersecurity experts can provide valuable perspectives on securing sensitive health/research data and protecting critical systems in these industries.

B. Women in tech and security

- **AI and Generative AI Threats:** Theresa Payton, former White House CIO and CEO of Fortalice Solutions, has highlighted the rise of AI-driven threats, including "Frankenfrauds" and deep fake AI personas. These threats involve sophisticated scams using AI to create realistic fake identities and scenarios, posing significant challenges for cybersecurity defenses. Payton emphasizes the need for robust security protocols and collaborative defense strategies to counter these emerging threats.
- **Human-Centric Cybersecurity:** Dr. Jessica Barker, co-founder and co-CEO of Cygenta, focuses on the human side of cybersecurity. She advocates for improving cybersecurity awareness, behaviors, and culture within organizations. Barker's work emphasizes the importance of understanding human psychology and sociology in cybersecurity, empowering individuals to recognize and mitigate cyber threats effectively. Her efforts include delivering awareness sessions and keynotes to large audiences, and authoring books on cybersecurity.
- **Cybersecurity Transformation and Organizational Culture:** Kirsten Davies, CISO at Unilever, is known for her expertise in cybersecurity transformation and enhancing organizational culture. She has led initiatives to refine security processes and improve ways of working across multiple global companies. Davies' approach involves optimizing security practices to align with business goals and fostering a culture of security within organizations.
- **Disaster Recovery and AI-Generated Threats:** Sarah Armstrong-Smith, Chief Security Advisor for Microsoft EMEA, has been instrumental in addressing disaster recovery, data protection, and privacy. She emphasizes the importance of considering information validity in decision-making, particularly in the context of AI-generated threats like deepfakes and mixed reality. Armstrong-Smith also highlights the need for organizations to stay ahead of evolving threats by leveraging AI and machine learning in their cybersecurity strategies.
- **Identity Threats and Influence Security:** Theresa Payton also discusses the evolving landscape of identity threats, including the potential for cybercriminals to hack into intelligent buildings and lock them down. She stresses the importance of understanding and mitigating these threats through innovative security measures and influence security strategies.
- **Diversity and Inclusion in Cybersecurity:** Lynn Dohm, Executive Director of Women in CyberSecurity (WiCyS), is a strong advocate for diversity and inclusion in the cybersecurity workforce. She highlights the importance of DEI policies in bridging the workforce gap and improving the recruitment, retention, and advancement of women in cybersecurity. Dohm's efforts aim to create a inclusive and effective security industry.

C. Women shaping the futrue AI

- **Mira Murati:** As the Chief Technology Officer at OpenAI, Mira Murati has been instrumental in the development and deployment of groundbreaking AI technologies such as ChatGPT, DALL-E, and Codex. Murati emphasizes the importance of public testing and responsible AI use, advocating for AI regulation to ensure that AI technologies align with human intentions and serve humanity positively. Her leadership has helped OpenAI become a leader in generative AI, pushing the boundaries of what AI can achieve while maintaining a focus on ethical considerations.
- **Linda Yaccarino:** Linda Yaccarino, CEO of X (formerly Twitter), is leveraging AI to enhance the platform's capabilities, particularly in the realm of fact-checking and content moderation. She has introduced Community Notes, a crowd-sourced fact-checking feature, which aims to improve the accuracy and trustworthiness of digital content. This initiative highlights the potential of AI to combat misinformation and enhance the credibility of online platforms.
- **Sarah Armstrong-Smith:** Sarah Armstrong-Smith, Chief Security Advisor for Microsoft EMEA, focuses on the intersection of AI and cybersecurity. She addresses the challenges posed by AI-generated threats such as deepfakes and emphasizes the importance of disaster recovery, data protection, and privacy. Armstrong-Smith advocates for the integration of AI in cybersecurity strategies to stay ahead of evolving threats, ensuring that AI technologies are used to enhance security and resilience.
- **Keren Elazari:** Keren Elazari, a security analyst and researcher, promotes the ethical use of AI and the hacker mindset to drive innovation in cybersecurity. She emphasizes the importance of ethical hacking and bug bounty programs to identify and mitigate AI-related vulnerabilities. Elazari's work in fostering a community of ethical hackers and her advocacy for increased representation of women in cybersecurity are crucial for developing robust AI security measures.
- **Catherine Lian:** Catherine Lian, General Manager and Technology Leader at IBM ASEAN, is at the forefront of AI integration in business. She stresses the need for upskilling workers to use AI effectively, ensuring that AI augments rather than replaces human jobs. Lian's efforts in promoting AI education and responsible AI governance are essential for building trust in AI technologies and preparing for future regulatory requirements.

D. Notable women, impact and the groundbreaking technologies across industries:

1) Maritime Industry:

Women are making significant strides in the maritime industry, particularly in enhancing cybersecurity measures. For example, initiatives like the International Maritime Organization (IMO) and the Women's International Shipping & Trading Association (WISTA) are actively promoting gender diversity and inclusion in maritime cybersecurity roles. These organizations emphasize the importance of cybersecurity in protecting shipboard and shore-based systems from cyber threats, and women are increasingly taking on leadership roles to drive these initiatives forward.

- **Tracy Edwards** - The first woman to lead an all-female crew in the Whitbread Round the World Race (now the Volvo Ocean Race) in 1989-1990.
- **Nennette Zande** - Developed the Aqua-Tractor, an amphibious vehicle used for beach cleanup and oil spill response.
- **Impact**: Women are leading efforts to secure maritime operations, protecting shipboard and shore-based systems from cyber threats.

2) Smart Cities:

In the realm of smart cities, women are contributing to the development and implementation of secure technologies. Anjana Rajan, a human rights technologist, is one such example, working on secure smart city solutions that integrate cybersecurity measures to protect interconnected systems. Women in this field bring unique perspectives that help address the diverse security needs of urban environments, ensuring that smart city infrastructures are resilient against cyber threats.

- **Anjana Rajan** - Works on secure smart city solutions, integrating cybersecurity measures to protect interconnected urban systems.
- **Ayah Bdeir** - Founder of littleBits, an open-source library of electronic modules that allows anyone to create prototypes and solutions for smart cities.
- **Impact**: Enhancing the resilience of urban infrastructures against cyber threats through innovative cybersecurity measures.

3) Railways:

The rail industry is seeing an increasing number of women contributing to cybersecurity. Marta, a Technical Affairs Manager at UNIFE, focuses on research, innovation, and cybersecurity in the rail sector. Her work involves developing strategies to protect rail systems from cyber threats, ensuring the safety and reliability of rail transport.

- **Mary Walton** - Designed the first industrial robot, the Unimate, which was used in automobile manufacturing and later adapted for railway maintenance.
- **Olga Trofimova** - Developed the first automated train control system, which improved railway safety and efficiency.
- **Impact**: Developing strategies to protect rail systems, ensuring the safety and reliability of rail transport.

4) Pharmaceutical/Biotech:

In the pharmaceutical and biotech industries, women are playing crucial roles in securing sensitive health and research data. For instance, cybersecurity measures in these industries are vital for protecting intellectual property and patient information from cyber threats. Women in cybersecurity roles within these

sectors are involved in developing and implementing robust security protocols to safeguard critical data and ensure compliance with regulatory standards.

- **Katalin Karikó** - Her work on mRNA technology laid the foundation for the development of mRNA vaccines, including the Pfizer-BioNTech and Moderna COVID-19 vaccines.
- **Tu Youyou** - Discovered artemisinin, a drug used to treat malaria, for which she was awarded the Nobel Prize in Physiology or Medicine in 2015.
- **Impact**: Implementing robust security protocols to protect intellectual property and patient information.

5) Cyberbiosecurity:

Cyberbiosecurity is an emerging field that combines cybersecurity with biological research and biotechnology. Women are at the forefront of this field, addressing the unique security challenges posed by the integration of digital and biological systems. Their contributions include developing strategies to protect bioinformatics data, securing biomanufacturing processes, and ensuring the integrity of biological research against cyber threats. Women in cyberbiosecurity are driving innovation and setting standards for securing the intersection of biology and technology.

- **Megan Palmer** - A pioneer in the field of cyberbiosecurity, she has contributed to developing strategies to secure bioinformatics data and protect biological research from cyber threats.
- **Diane DiEuliis** - Her work focuses on securing biomanufacturing processes and ensuring the integrity of biological products against cyber threats.
- **Impact**: Protecting bioinformatics data and biomanufacturing processes, ensuring the integrity of biological research.

III. Cybersecurity inclusive

A. How women's approaches differ from traditional cybersecurity strategies

The approaches led by women in cybersecurity often differ from traditional strategies in several keyways, emphasizing inclusivity, human-centric design, and the integration of diverse perspectives

- **Human-Centric and Inclusive Approaches:** Women in cybersecurity often advocate for a human-centric approach to cybersecurity. This involves considering the needs and experiences of all users, particularly marginalized groups, and ensuring that cybersecurity measures are inclusive and equitable. For example, the report by Hofstetter and Pourmalek emphasizes the importance of incorporating women's experiences and the knowledge of women's rights organizations into cybersecurity policies, advocating for a "whole-of-society" approach.
- **Gender-Sensitive Design and Policies:** Women in cybersecurity are pushing for gender-sensitive technology design and policies. This includes addressing the gendered implications of cybersecurity systems, processes, and practices. The report by the ICT4Peace Foundation highlights how technology design often misunderstands or omits gendered uses, leading to additional security burdens for women and other marginalized groups. This contrasts with traditional cybersecurity strategies that may overlook these gendered dimensions.
- **Diversity and Inclusion in Teams:** Women leaders in cybersecurity emphasize the importance of diversity and inclusion within cybersecurity teams. Diverse teams are seen as more effective in responding to a wide range of cyber threats due to their varied perspectives and experiences. For instance, the Check Point Software report notes that gender-diverse teams make better business decisions 73% of the time and are more creative in problem-solving. This focus on diversity contrasts with traditional cybersecurity teams, which have historically been male-dominated and less diverse.
- **Addressing Gender Norms and Stereotypes:** Charly Davis from Sapphire emphasizes the need for proactive strategies to attract diverse talent and improve mentorship opportunities for women in cybersecurity. This approach aims to break down barriers and create a more inclusive environment, differing from traditional strategies that may not explicitly address these issues.
- **Ethical and Responsible AI Use:** Murati from OpenAI advocates for AI regulation and public testing to align AI technologies with human intentions and serve humanity positively. This focus on ethical considerations and public accountability is a departure from traditional cybersecurity strategies that may prioritize technical solutions over ethical implications.
- **Holistic and Collaborative Defense Strategies:** Women in cybersecurity often promote holistic and collaborative defense strategies. This includes integrating AI and machine learning to enhance security measures and staying ahead of evolving threats. Sarah

B. Gender norms affect understanding of cybersecurity

Gender norms play a crucial role in shaping young adults' understanding of cybersecurity by influencing their perceptions, behaviors, and career choices. Addressing these norms through inclusive and gender-sensitive policies and education can help create a more equitable and effective cybersecurity landscape.

- **Influence of Gender Norms on Perceptions and Behaviors:** Gender norms shape individual identities, roles, and expectations within cybersecurity and broader society. These norms often associate technical expertise with men and masculinity, while communications expertise or equality initiatives are linked with women and femininity. This hierarchical social structure can lead to the undervaluation of contributions typically associated with women, affecting how young adults perceive and engage with cybersecurity.

- **Gendered Experiences and Cybersecurity Awareness:** Research indicates that gender affects cybersecurity awareness and behaviors. For instance, a study on Thai employees found that female employees had a higher level of cybersecurity awareness than their male counterparts. This suggests that gender norms and socialization processes might influence how different genders approach and prioritize cybersecurity.
- **Sociocultural Factors and Policy Implications**: The study comparing cybersecurity perceptions in Turkey and Italy highlights those sociocultural factors, including gender norms, significantly influence young adults' understanding of cybersecurity. These norms affect how young adults perceive cyber threats, their sense of security, and their responses to cyber dangers. The study emphasizes the need for gender-sensitive cybersecurity policies that consider these sociocultural dynamics to effectively address cybersecurity challenges.
- **Gender-Sensitive Cybersecurity Frameworks**: To address the gendered dimensions of cybersecurity, it is essential to implement gender-sensitive frameworks that consider the different experiences and needs of all genders. This includes mainstreaming gender perspectives into cyber norm implementation, providing gender-sensitive capacity building, and addressing the gender digital divide. Such approaches ensure that cybersecurity measures are inclusive and effective for everyone, regardless of gender.

C. Challenges in Integrating Gender Considerations into Cybersecurity Standards

Integrating gender considerations into cybersecurity standards faces several challenges:

- **Lack of Gender-Disaggregated Data:** There is a significant gap in gender-disaggregated data, which is crucial for understanding the specific cybersecurity needs and vulnerabilities of different gender identities. This lack of data makes it difficult to develop targeted and effective cybersecurity policies and standards.
- **Underrepresentation of Women and Gender Minorities:** Women and gender minorities are underrepresented in cybersecurity governance and decision-making processes. This underrepresentation means that their perspectives and experiences are often not considered, leading to policies and standards that may not address their specific needs.
- **Gendered Hierarchies and Biases:** Cybersecurity practices and standards often reflect gendered hierarchies and biases, prioritizing technical expertise (often associated with masculinity) over other forms of knowledge and participation. This can result in the devaluation of contributions typically associated with women and other marginalized groups.
- **Lack of Gender Mainstreaming**: Many existing cybersecurity standards and frameworks lack a systematic approach to mainstreaming gender considerations. This means that gender perspectives are not consistently integrated into the design, implementation, and evaluation of cybersecurity measures, leading to a failure to address the gendered dimensions of cybersecurity threats and practices
- **Resistance to Change and Lack of Awareness:** There may be resistance to incorporating gender considerations into cybersecurity standards due to a lack of awareness or understanding of the relevance of gender to cybersecurity. Some stakeholders may view gender as a peripheral issue rather than a central component of effective cybersecurity governance.
- **Complexity of Intersectionality:** Addressing gender in cybersecurity requires an intersectional approach that considers the intersections of gender with other factors such as race, class, age, disability, and sexuality. This complexity can make it challenging to develop comprehensive and inclusive standards.

D. Main Gendered Implications of Cybersecurity Practices

The gendered implications of cybersecurity practices are multifaceted and include:

- **Design and Technology:**
  - Cybersecurity technologies often inherit gender biases from their design processes. This can result in technologies that do not adequately protect women and marginalized groups or that place additional burdens on them.
  - Gender-sensitive design is crucial to ensure that cybersecurity tools are effective for all users, regardless of gender.
- **Defensive Measures:**
  - Defensive cybersecurity practices can reflect masculine norms, such as the emphasis on technical competence and autonomy. This can make it difficult for individuals to seek help or admit vulnerabilities, particularly in male-dominated environments.
  - Gender norms around vulnerability and cooperation can hinder effective cybersecurity defense, as individuals may be reluctant to work collaboratively or transparently.
- **Incident Response:**
  - The composition and culture of incident response teams can be influenced by gender dynamics. Teams that lack diversity may be less effective in addressing the full range of cyber threats and may perpetuate gender biases in their responses.
  - Informal networks and trust-based communities in cybersecurity can exclude women and marginalized groups, reducing their participation and influence in incident response efforts.

E. Gendered threat models

1) Gendered Threat Models Impact security Strategies

Gendered threat models significantly influence cybersecurity strategies by shaping how threats are perceived, prioritized, and addressed.

- **Differential Threat Perception:**
  - Gendered threat models often reflect societal biases, leading to the underrepresentation or misrepresentation of threats that disproportionately affect women and marginalized groups. For example, online harassment, cyberstalking, and non-consensual sharing of intimate images are more likely to be downplayed or omitted in traditional threat models.
  - This can result in cybersecurity strategies that do not adequately protect these groups, leaving them more vulnerable to specific types of cyber threats.
- **Additional Security Burdens:**
  - Women and marginalized groups may face additional security burdens due to gendered threat models. For instance, they might need to adopt more robust privacy measures or take extra precautions to protect their online identities, which can be time-consuming and costly.
  - Cybersecurity strategies that do not account for these additional burdens can inadvertently place a heavier load on these groups, exacerbating existing inequalities.
- **Disingenuous Cybersecurity Marketing:**
  - Gendered threat models can also influence the marketing of cybersecurity technologies. Products may be advertised in ways that do not resonate with or address the specific needs of women and marginalized groups, leading to lower adoption rates among these populations.
  - Effective cybersecurity strategies should include marketing approaches that are inclusive and consider the diverse needs of all users

2) Gender Stereotypes Influence Threat Simulations

Gender stereotypes play a significant role in shaping cybersecurity threat simulations, impacting both the design and execution of these exercises:

- **Stereotypical Characterizations:**
  - Threat simulations often involve gender stereotyping, where roles and scenarios are based on traditional gender norms. For example, men might be depicted as the primary defenders or attackers, while women are portrayed in less technical or supportive roles.
  - This can reinforce gender biases and limit the perceived capabilities of women and other marginalized groups in cybersecurity roles.
- **Norms of Masculinity in Defense:**
  - The concept of defense in cybersecurity is often associated with norms of masculinity, such as technical competence, autonomy, and protection. These norms can make it difficult for individuals to admit errors, seek help, or work cooperatively, which are essential for effective cybersecurity defense.
  - Gender norms around vulnerability can hinder transparency and collaboration, leading to less effective threat simulations and real-world responses.

3) Gendered threat models. Phishing scenarios

Gendered threat models can significantly influence the approach to phishing simulations, leading to differences in how these simulations are designed, executed, and evaluated.

- **Threat Prioritization:**
  - Traditional threat models often prioritize phishing attacks that target financial or corporate data, which may overlook threats more commonly faced by women and marginalized groups, such as online harassment, cyberstalking, and non-consensual sharing of intimate images.
  - Phishing simulations based on these traditional models may fail to adequately represent the specific social engineering tactics used in gender-based cyber threats.
- **Scenario Design:**
  - Phishing simulations often involve gender stereotyping in the roles and scenarios depicted, reinforcing traditional gender norms.
  - Men might be portrayed as the primary defenders or attackers, while women are depicted in less technical or supportive roles.
  - Such stereotypical characterizations can reinforce gender biases and limit the perceived capabilities of women and other marginalized groups in cybersecurity roles.
- **Participant Selection:**
  - The composition of participants in phishing simulations may be influenced by gender dynamics, potentially leading to an underrepresentation of women and marginalized groups.
  - This can result in simulations that fail to capture the diverse experiences and vulnerabilities faced by different gender identities.
- **Evaluation Metrics:**
  - Traditional phishing simulations often evaluate success based on metrics such as click-through rates or data exfiltration, which may not adequately capture the impact of gender-based cyber threats.

- Gendered threat models may require different evaluation metrics that consider the psychological and social impacts of phishing attacks on different gender identities.

- **Defensive Strategies:**
  - Defensive strategies taught in phishing simulations can reflect masculine norms, such as an emphasis on technical competence and autonomy.
  - This can make it difficult for individuals to seek help, admit vulnerabilities, or work collaboratively, which are essential for effective cybersecurity defense.

- **Incident Response:**
  - The composition and culture of incident response teams involved in phishing simulations can be influenced by gender dynamics.
  - Teams that lack diversity may be less effective in addressing the full range of cyber threats and may perpetuate gender biases in their responses

To address these issues, it is crucial to incorporate gender-sensitive approaches into phishing simulations.

- Developing threat models that consider the unique vulnerabilities and experiences of different gender identities.
- Ensuring diverse and inclusive participant selection and scenario design.
- Evaluating simulations based on metrics that capture the psychological and social impacts of gender-based cyber threats.
- Promoting defensive strategies that emphasize collaboration, transparency, and support-seeking behaviors.
- Fostering diversity and inclusivity within incident response teams involved in phishing simulations.

4) Best Practices for Gender-Sensitive Cybersecurity Training

To address these challenges and create more inclusive cybersecurity strategies, the following best practices for gender-sensitive cybersecurity training are recommended:

- **Inclusive Curriculum Design:** Develop training materials that address the specific cybersecurity threats faced by different gender identities. Include case studies and scenarios that reflect the diverse experiences of women, men, and non-binary individuals.
- **Gender-Sensitive Threat Modeling:** Incorporate gender-sensitive threat modeling into training programs. Ensure that threat models consider the unique vulnerabilities and security needs of all gender identities.
- **Promote Diversity and Inclusion:** Encourage the participation of women and marginalized groups in cybersecurity training programs. Create a supportive and inclusive learning environment that values diverse perspectives and experiences.
- **Address Gender Biases and Stereotypes:** Provide training on recognizing and addressing gender biases and stereotypes in cybersecurity practices. This includes challenging traditional norms of masculinity and promoting a culture of transparency and collaboration.
- **Collaborate with Civil Society and Academia:** Work with civil society organizations and academic institutions to develop comprehensive and intersectional cybersecurity training programs. These collaborations can help ensure that training materials are informed by the latest research and best practices in gender-sensitive cybersecurity.
- **Continuous Monitoring and Evaluation:** Implement mechanisms for continuous monitoring and evaluation of cybersecurity training programs to ensure they remain inclusive and effective. Collect feedback from participants and make necessary adjustments to address any gaps or biases.