01. Introduction
This paper explores cybersecurity education prevalence, availability, and application. Cybersecurity education is the process of teaching individuals and organizations the knowledge and skills needed to protect computer systems, networks, and data from cyber threats and attacks. A cyber threat is a potential malicious attack aimed at accessing, altering, or destroying sensitive data, disrupting digital operations, or causing harm to digital systems, often originating from hackers, cybercriminals, or other malicious entities. Small and Medium-Sized Enterprises (SMEs) are classified as businesses with fewer than 250 employees and revenue not exceeding 50,000,000 dollars.

Background
- In 2020, only 14% of American SMEs had a cybersecurity framework in place, allowing 700,000 attacks that resulted in $2.8 billion in damages
- SME’s lose an average of $25,000 annually on cyber attack damages
- 73% of UK SMEs described trouble accessing cybersecurity education materials, 1/3 of UK SMEs did not consider Cyber-attacks and data a significant risk
- The primary threats to SME’s are malware attacks, phishing, insider attack, web attacks, ransomware, compromised servers, and malicious emails.

02. Objective
Identify the key challenges faced by small businesses in implementing cybersecurity practices, promote resources to help them deal with cybersecurity threats, evaluate the benefit of cyber-education for SMBs, and mitigate cyber threats.

03. Methodology
- **Databases**: IEEE, ACM Digital Library, Web of Science, Elsevier
- **Keywords**: cybersecurity awareness, education, Small or Medium Business
- **Number of articles**: The initial was 339 articles, and the final included articles were 25 articles.
- **Analysis**: Identified cybersecurity frameworks used and recommendations for SMEs and SMBs.

04. What Research Recommends
Results of what frameworks we recommend weighing ease, accessibility, and price.

1. NIST Cybersecurity Framework
   - a. Flexible framework, easily adapted to specific SMB needs, budget, and because of limited resources
   - b. Enhances credibility and compliance with industry standards as it is widely recognized and accepted

2. ISO 27001
   - a. This certification is very structured, includes risk assessment, and continually improves.
   - b. Certification is scalable and can be implemented in increments at a SMBs pleasure or capacity.

3. Cloud Security Services (the ones here are free)
   - a. Google Workspace
     - i. Phishing protection, malware detections, encryption available for emails and files
     - ii. Secure cloud storage and management tools are present through Google Drive.
     - iii. Can be accessed and used on mobile version as well for convenience, has built-in version history so data is saved.
   - b. Microsoft 365
     - i. Secure collaboration features such as file sharing.
     - ii. Encrypts data in transit and in rest for protection.
     - iii. Includes Azure Active Directory for identity and access management for user identity and access control management.

Both Cloud Security Services comply with industry standards such GDPR and HIPPA for sensitive information.

05. Analysis
This bar graph is showing the popularity of each framework by evaluating which ones are implemented by SMEs. We can see implementing no frameworks is most frequent at just under 50% and the most popular framework being ISO 27001.

06. Conclusion
SMEs often lack cybersecurity frameworks due to funding and leadership support issues. Many lack updated cyber-risk strategies due to budget concerns. This leads to neglect in security training and culture. Perceived high costs also deter adoption, despite affordable security measures available: training staff, updating systems, using free tools, and creating response plans boost security without major expenses.

07. Acknowledgements
This work is supported by funding for the VICEROY Northwest Institute for Cybersecurity Education and Research (CySER) provided by the Office of the Undersecretary of Defense for Research and Engineering in collaboration with the Air Force Research Laboratory and Griffiss Institute.

08. References

Bridging the Cybersecurity Awareness Gap in Small and Medium-sized Enterprises: Challenges, Solutions, and Future Directions
Meredith Lamb, Jessica Martin & Blessing Akinrotimi