Risks to Critical Infrastructure in Hawaii - A Small Business Perspective

Debasis Bhattacharya
University of Hawaii Maui College
debasisb@hawaii.edu

Una Bella
University of Hawaii Maui College
unabella@hawaii.edu

Angelo Bella
University of Hawaii Maui College
angelo8@hawaii.edu

ABSTRACT

This lightning talk addresses the pressing need to enhance cybersecurity measures for Hawaii's critical infrastructure, focusing particularly on healthcare and transportation sectors. These sectors have faced significant cybersecurity challenges, with Oahu's transportation services experiencing major breaches and healthcare institutions like Queen's Health System and Malama I Ke Ola suffering from ransomware attacks since 2021. These incidents have led to severe disruptions and compromised sensitive data. Hawaii's geographic isolation, natural disaster risks, legacy systems, and workforce shortages exacerbate these issues. Additionally, emerging technologies such as AI and IoT further expand vulnerabilities. A comprehensive cybersecurity strategy is essential to mitigate these risks. This talk introduces the concept of a volunteer-supported Human-AI Synergy Hotline, which provides proactive advice, crisis management, and emotional support during and after cyber incidents. This innovative approach aims to enhance cybersecurity preparedness and resilience in Hawaii's critical sectors.

ACM Reference Format:
Debasis Bhattacharya, Una Bella, and Angelo Bella. 2024. Risks to Critical Infrastructure in Hawaii - A Small Business Perspective. In *The 25th Annual Conference on Information Technology Education (SIGITE '24), October 10–12, 2024, El Paso, TX, USA.* ACM, New York, NY, USA, 1 page. https://doi.org/10.1145/3686852.3686883

1 INTRODUCTION

Hawaii's healthcare and transportation sectors are critically vulnerable to cybersecurity threats, underscoring the urgent need for robust measures to defend against targeted attacks and prevent collateral damage [1]. The geographic isolation and natural disaster risks create a vulnerable foundation compounded by legacy systems and workforce shortages. Emerging technologies like AI and IoT expand vulnerabilities across critical infrastructure. The threat landscape includes ransomware, supply chain attacks, and other forms of cyber threats, impacting vital services and revealing cascading effects through interconnected systems [2, 3]. The rapid adoption of telehealth has introduced new data privacy concerns, necessitating a comprehensive cybersecurity strategy that addresses both digital and physical vulnerabilities [4, 5].

Cultivating a robust cybersecurity culture is crucial for risk mitigation. This approach emphasizes awareness of social engineering tactics and strong cyber hygiene practices, complemented by technical measures such as zero trust models, regular updates, encryption, and endpoint protection [6]. Ongoing awareness programs equip staff to recognize phishing attempts and maintain proper data handling protocols. Multi-factor authentication and biometric verification reinforce access controls. This integrated strategy strengthens Hawaii's cyber defenses by addressing both human and technical vulnerabilities.

The proposed free community cyber clinic and hotline, operated by volunteers who are human experts and augmented by AI, offers proactive advice and crisis management. It provides guidance on software updates, multi-factor authentication, and best practices. During cyber incidents, it delivers immediate expert help and emotional support, ensuring personnel remain calm and effective. This human-AI team is modeled after public health support systems prevalent during the Covid pandemic, ensuring a personalized support mechanism through human volunteers available via chat or phone, as well as AI agents that continuously learn about the latest cybersecurity threats and vulnerabilities.

Many individuals are susceptible to social engineering due to a lack of basic cybersecurity knowledge. For those unsure where to start, a free cyber clinic and human-guided hotline offers clear instructions and follow-up. This demystifies the process, reassuring users that technology and AI are supportive tools. Combined human and AI support offers practical solutions, empowering individuals to confidently mitigate cyber threats.

REFERENCES

[1] Guzman, N. H. C., *et al.* (2021). Vulnerabilities in maritime transportation systems and resilience strategies: A systematic review. Transportation Research Procedia, 55, 1552-1559.
[2] Cybersecurity and Infrastructure Security Agency. (n.d.). Transportation Systems Sector. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/transportation-systems-sector.
[3] Positive Technologies. (2023). Cybersecurity threats cape in the transport sector: 2023. https://www.ptsecurity.com/ww-en/analytics/cyber-threats-in-the-transport-sector-2023/
[4] Hawaii News Now. (2024). Maui Health Center allegedly attacked by Russian hackers. https://www.hawaiinewsnow.com/2024/06/20/maui-health-center-allegedly-attacked-by-russian-hackers
[5] Health-ISAC. (n.d.). Feds warn healthcare sector of Maui ransomware threats. https://h-isac.org/feds-warn-healthcare-sector-of-maui-ransomware-threats/.
[6] U.S. Department of Health and Human Services. (2024, March 5). HHS Statement Regarding the Cyberattack on Change Healthcare. https://www.hhs.gov/about/news/2024/03/05/hhs-statement-regarding-the-cyberattack-on-change-healthcare.html.

SIGITE '24, October 10–12, 2024, El Paso, TX, USA

ACM ISBN 979-8-4007-1106-0/24/10
https://doi.org/10.1145/3686852.3686883