**CYBR 450**

**Abby Gopal**

**Week # 5**

**Business Report**

**The Ransomware Attack on Our Granite Stone Business**

Khan, I., & Rahman, M. (2023). An assessment of cybersecurity practices in small businesses: A case study approach. *Asian Journal of Contemporary Education*, 7(1), 45-57. <https://www.ajpojournals.org/journals/index.php/AJCE/article/view/1906/2212>

**Annotation:**

This article explores cybersecurity practices among small businesses, using a case study approach to identify common vulnerabilities and effective mitigation strategies. The authors emphasize the importance of adopting robust cybersecurity measures, including employee training and incident response plans. This source is particularly pertinent to our granite stone business, providing actionable insights into improving cybersecurity practices and protecting against threats like ransomware.

**Citation:**

*Protecting Against Cyber Threats to Managed Service Providers and their Customers | CISA*. (2022, May 11). Www.cisa.gov. <https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-131a>

**Annotation:**

This publication from the Cybersecurity & Infrastructure Security Agency (CISA) details the various cyber threats that Managed Service Providers (MSPs) face and the implications these threats have for their clients. It discusses prevalent attack methods, including ransomware and phishing, and emphasizes the significance of MSPs in the overall cybersecurity landscape. The document provides actionable recommendations for MSPs and their customers, including adopting strong security practices, conducting thorough security assessments, and developing robust incident response strategies. This resource is crucial for understanding how to effectively collaborate with MSPs to enhance cybersecurity measures, especially relevant to our granite stone business, which seeks to protect sensitive data and ensure compliance with regulatory frameworks.

**Citation:**

Boyle, R. J., & Panko, R. R. (2021). *Corporate Computer Security* (5th ed.). Pearson Higher Ed. <https://platform.virdocs.com/read/2228243/1/#/4>

**Annotation:**

This textbook provides a thorough exploration of cybersecurity principles, with a focus on corporate settings. It discusses various forms of cyber threats, including ransomware attacks and phishing schemes, and offers best practices for prevention and response. The text emphasizes the importance of comprehensive employee training, robust security policies, and incident response plans. This foundational resource will support the development of strategies to enhance the cybersecurity posture of our granite stone business following the recent ransomware attack.

**Citation**

Todt, K. E. (2019). Data privacy and protection: What businesses should do. *The Cyber Defense Review, 4*(2), 39–46. <https://www.jstor.org/stable/26843891>

**Annotation**

Todt discusses essential strategies businesses must adopt to safeguard data privacy and protection in this article. The author outlines key principles, including the importance of risk assessment, data minimization, and establishing clear privacy policies. Additionally, the article emphasizes the need for employee training and awareness to prevent data breaches, especially in the context of evolving cyber threats. This source is particularly relevant to our granite stone business as it offers actionable insights on enhancing data protection measures, which is crucial following the recent ransomware attack that exposed sensitive customer and financial data.

**Citation:**

Verma, Ritesh. (2024). CYBERSECURITY CHALLENGES IN THE ERA OF DIGITAL TRANSFORMATION. 10.25215/9392917848.20. <https://www.researchgate.net/publication/377625512>

**Annotation:**

In this book, Dr. Ritesh Verma explores the multifaceted cybersecurity challenges that arise from rapid digital transformation across various industries. The author discusses issues such as data privacy, the rise of sophisticated cyber threats, and the importance of adopting a proactive cybersecurity posture. With a focus on strategic frameworks and best practices, this resource is crucial for understanding the broader context of cybersecurity, particularly in relation to the ransomware attack on our granite stone business. It will provide valuable insights into building a resilient security infrastructure and navigating the complexities of digital transformation.

Baltuttis, D., & Teubner, T. (2024). *Effects of visual risk indicators on phishing detection behavior: An eye-tracking experiment*. Https://Www.sciencedirect.com/Science/Article/Pii/S0167404824002451?Via%3Dihub. <https://doi.org/10.1016/j.cose.2024.103940>

**Annotation:**

This study explores how visual risk indicators, such as warning symbols and alerts, affect users' ability to detect phishing attempts. Using eye-tracking technology, the researchers measured participants' attention to these visual cues and their effectiveness in improving phishing detection. The results show that visual risk indicators significantly improve user awareness, especially for individuals with less cybersecurity experience. This article is highly relevant for our granite stone business, as it supports the idea that well-designed visual cues in emails and web interfaces can enhance employees' ability to detect phishing, reducing the risk of future ransomware attacks. This source will aid in developing user-friendly phishing detection mechanisms as part of our broader cybersecurity training efforts.