CHAPTER IV
CONCLUSIONS AND RECOMMENDATIONS

4.1 Conclusion

Based on the findings derived from the analysis of factors affecting customer loyalty following the cyber attack on Bank Syariah Indonesia (BSI), several conclusions can be drawn:

1. Perceived Risk Influence on Customer Loyalty: The study confirms a significant positive relationship between perceived risk and customer loyalty. This underscores that heightened perceptions of risk post-cyber attack diminish customer loyalty to BSI. Customers' concerns and uncertainties regarding data security contribute to their reduced loyalty to the bank.
2. Customer Trust's Impact on Customer Loyalty: The research establishes a significant positive association between customer trust and loyalty. This indicates that higher levels of trust in BSI's ability to safeguard data and address cyber threats correlate with increased customer loyalty. Customer trust serves as a crucial foundation for fostering long-term loyalty, particularly in contexts involving financial information security.
3. Perceived Risk's Effect on Customer Trust: The findings reveal a significant positive relationship between perceived risk and customer trust. Despite initial expectations, heightened perceptions of risk following a cyber attack can paradoxically enhance customer trust in BSI. Transparency and effective risk management strategies by the bank contribute to strengthening customer trust amidst heightened risk perceptions.
4. Service Quality's Impact on Customer Loyalty: Surprisingly, the study does not find a significant influence of service quality on customer loyalty post-cyber attack. This suggests that while service quality is important for customer satisfaction, other factors such as perceived risk and customer trust may exert a stronger influence on loyalty in the aftermath of a cyber attack.
5. Service Quality's Effect on Customer Trust: The research establishes a significant positive relationship between service quality and customer trust. High-quality service provision

by BSI contributes to bolstering customer confidence in the bank's ability to mitigate cyber attacks and protect customer information. Consistent delivery of reliable and satisfactory services strengthens customer trust in the institution.

6. Mediating Role of Customer Trust: The study confirms the mediating role of customer trust in the relationships between perceived risk and customer loyalty, as well as between service quality and customer loyalty. Customer trust emerges as a critical mediator through which perceived risk and service quality indirectly influence customer loyalty post-cyber attack. Strengthening customer trust is therefore essential for mitigating the negative impact of perceived risk and enhancing the positive impact of service quality on customer loyalty.
7. Mediating Role of Perceived Risk in Customer Loyalty: The research findings highlight the mediating role of perceived risk in the relationship between service quality and customer loyalty. Although service quality alone may not directly influence customer loyalty post-cyber attack, the study reveals that perceived risk acts as a mediator in this relationship. Customers' heightened perceptions of risk, stemming from the cyber attack, can diminish the impact of service quality on loyalty. Therefore, effectively managing perceived risk is crucial for maximizing the positive impact of service quality on customer loyalty. Strengthening risk mitigation strategies and fostering transparency can help mitigate the negative influence of perceived risk, thereby enhancing the effectiveness of service quality in maintaining customer loyalty.

In summary, the findings underscore the importance of factors such as customer trust, perceived risk, and service quality in shaping customer loyalty following a cyber attack on Bank Syariah Indonesia. The study highlights the need for BSI to prioritize transparency, effective risk management, and continuous service improvement to mitigate risk perceptions, enhance customer trust, and ultimately strengthen customer loyalty in the aftermath of cyber security incidents.

4.2 Recommendations

4.2.1 Proactive Risk Mitigation

Given the significant influence of perceived risk on customer loyalty post-cyber-attack, Bank Syariah Indonesia (BSI) should prioritize proactive risk mitigation efforts. This

entails investing in robust cybersecurity measures and incident response strategies to minimize perceived risk levels among customers. By demonstrating a commitment to security and actively addressing potential threats, BSI can help alleviate customer concerns and maintain trust.

4.2.2 Continuous Service Improvements

Considering the pivotal role of service quality in influencing customer loyalty, BSI should focus on continuous service improvement initiatives. Despite cybersecurity challenges, the bank should remain dedicated to delivering high-quality services that meet and exceed customer expectations. By consistently enhancing service standards and ensuring a seamless customer experience, BSI can strengthen customer loyalty even in the aftermath of a cyber-attack.

4.2.3 Trust-Building Initiatives

Recognizing the importance of customer trust as a mediator in the relationship between perceived risk, service quality, and loyalty, BSI should implement targeted trust-building initiatives. Transparent communication about security measures, personalized customer support, and timely resolution of security issues are essential for fostering trust and loyalty among customers. BSI should prioritize initiatives aimed at building and maintaining trust, particularly in the aftermath of security breaches.

4.2.4 Employee Training and Awareness

To reinforce its cybersecurity defenses and enhance customer trust, BSI should invest in comprehensive employee training and awareness programs. Well-trained employees play a crucial role in identifying and mitigating cyber threats, thereby safeguarding customer data and preserving trust. By educating employees about cybersecurity best practices and fostering a culture of vigilance, BSI can strengthen its overall resilience against cyber-attacks

4.2.5 Collaboration and Knowledge Sharing

Given the interconnected nature of cybersecurity threats, BSI should actively engage in collaboration and knowledge sharing initiatives with industry partners, regulatory bodies, and cybersecurity experts. By sharing insights and best practices for enhancing resilience, BSI can stay ahead of emerging threats and better protect its customers' interests. Collaborative efforts can yield valuable learnings and contribute to the collective cybersecurity resilience of the banking sector.

4.2.6 Adaptability in Crisis Management

In response to the cyber-attack, BSI should focus on enhancing its crisis management capabilities. This includes establishing clear protocols for incident response, communication, and recovery efforts. By adopting an agile and adaptive approach to crisis management, BSI can minimize the impact of cyber-attacks on customer loyalty and organizational reputation.

4.2.7 Continuous Customer Engagement

Following a cyber-attack, BSI should prioritize continuous engagement with customers to address concerns and rebuild trust. This involves proactive communication, regular updates on security measures, and soliciting feedback to improve customer experience. By maintaining open channels of communication and demonstrating a commitment to customer-centricity, BSI can reinforce customer loyalty and resilience in the face of cybersecurity challenges. By implementing these recommendations, BSI can effectively address the challenges posed by cyber-attacks, maintain customer loyalty, and emerge as a trusted and resilient institution in the banking sector.