INSPIRA: Indonesian Journal of Psychological Research
https://journal.iainlangsa.ac.id/index.php/inspira

RESEARCH ARTICLE

Cyber resilience in combating ransomware attacks: A psychological case study perspective on the hospitality industry

https://doi.org/10.32505/inspira.v5i2.9618

Yenika Putri Cahyandari[1], Tutut Chusniyah[2] Ninik Setiyowati[3]

[1] Department of Psychology, State University of Malang, East Java, Indonesia
[2] Department of Psychology, State University of Malang, East Java, Indonesia
[3] Department of Psychology, State University of Malang, East Java, Indonesia

Corresponding Author:
Yenika Putri Cahyandari (email: yenika.putri.2308118@students.um.ac.id)

ABSTRACT

This paper studies the drivers that have a significant impact on organizational resilience in terms of ransomware attacks in the hospitality industry of Indonesia, with a particular focus on hotels operating in Bali. The interviews with IT managers in two of the most important hotels were conducted using in-depth interviews. They showed that the ransomware attacks caused severe operational disturbances and a loss of consumer confidence. Despite these, several proactive measures have been put in place by the hotels, and this has emanated through the strong leadership from the senior management to upgrade cybersecurity infrastructure and to instigate staff awareness programs. The findings pinpoint budget limitations and inadequate training, which align with the existing literature, as some of the important obstacles. The work underlines the desperate need for adaptive strategies in cybersecurity and develops an understanding that a collective organizational commitment is required toward sensitive data protection and good reputation building. Indeed, the research points out that creating security awareness among all employees would genuinely enhance the culture of cybersecurity and resilience. Collaboration between industry players and governmental bodies may provide the required wherewithal and frameworks for building up strength with which the ransomware threat could be tackled effectively. Given the practical recommendations, it might be useful to consider how to make the hospitality industry resilient in the case of ransomware attacks.

Article History:
Received 12 October 2024
Revised 21 December 2024
Accepted 31 December 2024

Keywords: *case study; cyber psychology; hospitality industry; ransomeware; resilience*

INTRODUCTION

Ransomware attacks have been increasing over the past couple of years and thus are considered a significant threat to various industries, including hospitality. Indeed, according to a study by Data Protection Research, "as many as 74% of companies in the hospitality industry experienced

How to cite (APA 7th Edition)
Cahyandari, Y. P., Chusniyah, T., & Setiyowati, N. (2024). Cyber resilience in combating ransomware attacks: A psychological case study perspective on the hospitality industry. *INSPIRA: Indonesian Journal of Psychological Research, 5*(2), 216–229. https://doi.org/10.32505/inspira.v5i2.9618

cyberattacks over the past two years, with 45% reporting significant financial losses due to ransomware attacks" (Connolly et al., 2020). In that respect, ransomware attacks will break operational efficiency, reputation, and customer trust. A ransomware attack on the hotel reservation system leads to a loss of customer data and disruption in the service, and the business losses are enormous. Law et al. (2013) indicated that hospitality remains an attractive target since most properties depend on integrated and complex information technology systems; these are likely to have security vulnerabilities that could be exploited. As indicated, the organization is at risk of cyberattacks, including ransomware, in the hospitality industry, which is deeply dependent on information technology. Property management systems, online booking systems, and customer service applications require tight security so unauthorized people cannot access them. Most hospitality organizations have weak cybersecurity strategies, which have recently been under a massive attack (Cobanoglu et al., 2021). Poor cybersecurity not only puts sensitive data in jeopardy but also hamper the trust of consumers and hurt the business.

Attacks involving ransomware have significantly increased in recent years, causing a high threat for many industries, including the hospitality industry. According to a survey conducted by Ell (2024), 74% of hospitality companies have been subjected to cyberattacks in the past two years, while 45% of ransomware attacks resulted in considerable financial loss for their business. In this context, ransomware attacks can significantly impact operations, reputation, and consumer trust. For example, suppose reservation systems in hotels are attacked by ransomware. In that case, the attack quickly leads to the inability to access consumer data and disruptions in services, hence, substantial financial losses for the business. Moreover, Florido-Benítez (2024) explains that the main targets include the hospitality industry since integrated information technology systems are widely used but with high levels of complexity, which commonly have security vulnerabilities to take advantage of. In the wake of ransomware attacks, organizational resilience in the digital era is becoming critical. Resilience would, therefore, involve not just the prevention and detection of the attack but the response and quick recovery from the attack. A study by Aqilah et al. (2024) established that organizations with well-structured incident response plans can significantly reduce the adverse impacts of ransomware attacks. This research underlines a holistic approach to cybersecurity management, including employee training, robust security policies, and advanced technologies.

The Indonesian hospitality industry is not excluded from the threat of ransomware attacks. A study conducted by Yanuarni et al. (2024) has shown that many hotels in Indonesia still have poor awareness of the importance of cybersecurity and organizational resilience. Two main obstacles to developing resilience effectively are insufficient investment in cybersecurity infrastructure and a lack of employee training. This is further aggravated by the fact that, in most countries, there are not enough strict regulations or governmental controls to ensure adequate protection of customer data in the hospitality industry. Given the recent growth of ransomware attacks over the last few years, significant importance has to be attributed to the role of organizational resilience in ensuring business continuity in the hospitality industry. These findings are supported by the study featured in the Journal of Cybersecurity, in which the authors said, "Resilience against cyberattacks is a critical element in business sustainability strategies within the hospitality sector, in particular considering its high dependence on information technology systems" (Safitra et al., 2023). Indeed, it is shown by Alawida et al. (2022) that hotels that can incorporate cybersecurity strategies into their daily operations successfully turn out to be far more effective in countering ransomware attacks with minimal losses. This would encompass the implementation of robust security protocols, periodic updating of systems, and continuous education of staff about cyber threats.

At the heart of this research is the problem statement: developing resilience in the hospitality industry in Indonesia against ransomware attacks. This research attempted to investigate the potential vulnerabilities of existing cybersecurity strategies and recommend ways hotels can enhance their capacity for preventing, detecting, responding to, and recovering from incidents. Although several studies have been conducted on organizational resilience and cybersecurity within the hotel industry, the context has always differed from that of Indonesia. This study attempts to find the significant factors affecting organizational resilience against ransomware attacks in Indonesia's hospitality industry. It points out weaknesses in current cybersecurity strategies utilized by hotels within the country. Recommendations based on these findings may improve their capabilities in deterring, detecting, responding to, and recovering from ransomware attacks. The significance of this study is in its contribution to the cybersecurity of the hospitality industry and organizational resilience (Appiah et al., 2022; Gundu & Mmango, 2024; He et al., 2023; Marcucci et al., 2022). This research tries to increase awareness and improve the ability of hotels to respond to this threat through an in-depth analysis of strategies and best practices in countering ransomware attacks, which are applied to the challenges at hand.

The research has combined several theoretical frameworks to construct the study's framework. In this regard, a better understanding of the underlying principles leading to the research could be elicited. This would help ensure that the outcome is deeply rooted in established academic discourses by increasing the scope and depth of analysis. Only this complex theoretical integration will provide a nuanced understanding of the subject matter for further scholarly contribution to the research.

Organizational Resilience Theory

In this regard, the theory of organizational resilience provides perhaps one of the most important bases on which the depth of a hotel's ability to survive such an incident as a ransomware attack can be examined (Vogus & Sutcliffe, 2007). Based on this theory, organizational resilience indicates how business organizations can anticipate, prepare for, respond, adapt, and recover from disruptive events. In this research, it is important to assess the strength of a hotel's security protocols, the frequency with which a hotel updates systems, the comprehensiveness of its employee training, and the effectiveness of incident response plans. The examination is meant to provide the strengths and weaknesses of hotel resilience to pinpoint areas where further improvements should be made in actual ransomware incident prevention, detection, and management strategies. Additionally, implementing best practices based on organizational resilience theory is bound to contribute to a hotel's overall resilience against cyberattacks. The elements in this study will be critically analyzed to contribute to the knowledge base relating to the most efficient mechanisms for ensuring resilience in the hospitality industry and, consequently, an atmosphere of safety coupled with continuity of operations.

Ransome Risk Theories

The ransomware vulnerability theories explain why the hospitality industry has emerged as a soft target for ransomware attacks due to its dependency on integrated information technology systems (Al-rimy et al., 2018). Because of its compelling reliance on complex, virtually interrelated technologies, it has become exceptionally easy to use as an avenue for hackers with ransomware intentions (Cartwright et al., 2019). It considers several factors in ransomware risk theories, including insufficient cybersecurity protocols, a lack of investment in security infrastructure, and an absence of comprehensive staff training. Each one of these factors contributes to increasing the vulnerability. It, therefore, seeks to critically assess the impact of these factors on the risk of ransomware to hotels and, in the process, generates a detailed understanding of the peculiar challenges experienced within

this industry. Moreover, this research points out the best practices that need fortification to reduce vulnerabilities efficiently based on propositions of ransomware risk theories. This, in turn, will help develop targeted strategies for improving the cybersecurity posture of the hospitality industry as a whole and making it resilient against the upcoming threats of ransomware attacks. This will go a long way in informing future policy and operational decisions within the industry about how technology integrations interact with cybersecurity.

Situational Crime Prevention Theory

The situational crime prevention theory states that crimes can be minimized by strategies that avoid criminal opportunities like those around ransomware attacks (Clarke, 1980). This theory postulates that through continuous discouragement of the effort in committing the crime and, while at it, reducing the reward or benefits derived from committing the same offenses, the incidences of the same can be grossly reduced. On this basis, specific proactive steps in the line of ransomware can be done to effect anticipatory actions regarding the theory by increasing cybersecurity measures, targeting personnel training, establishing formal response mechanisms to incidents, accordingly increasing the offender hurdle, and reducing the offender reward. The scope of this research will be to determine the level of hotel compliance with situational crime prevention theory principles and, simultaneously, gauge the extent of its infusion that would improve resilience against ransomware attacks. From the idea behind the situational crime prevention theoretical framework, an analysis of today's security practices will determine the future implications regarding vulnerability to cybercrime. Therefore, this would contribute to the literature with empirical evidence regarding the efficacy of situational crime prevention strategies against cybercrime threats that are invariably changing, giving insight that stakeholders can use in upgrading their security measures.

METHOD

This study adopts the qualitative research approach, where the researcher aims to explore the details of the studied phenomenon by collecting qualitative data in a structured manner (Braun et al., 2017). This approach allows for a deep analysis of the subject of study and complete acquaintance with all subject dimensions. He does this through interviews, focus groups, and participant observation to obtain rich, descriptive data that sheds light on the intricacies of the particular case. This qualitative study does not merely attempt to record the present realities but also hopes to come up with findings that may add to the growing academic discussion of the topic.

The researcher identifies this study as one adopting a case study design. In such research, the investigator collects in-depth data on a specific ongoing case near the researcher (Wirza, 2018). This kind of research design enabled the researcher to explore the details and nuances of the case under consideration to understand the case's context, dilemmas, and implications. This design shall be suitable for capturing the intricacy of situations existing in real life, and valuable qualitative information can also be grasped, which might help explain the broader area of study. The insights drawn from this investigation may offer valuable input in future research and practical applications regarding the phenomenon under scrutiny.

The study also involves IT managers from two of Bali's leading hotels. The two were selected based on their extensive experience and the IT team's practices in the respective hotels. The reason for their selection is that there was a need to seek an understanding from individuals with in-depth insight into the hospitality industry’s unique technological challenges and opportunities. Through this qualitative research approach, targeting professionals with extensive experience, an attempt would be made to establish how IT strategies could be effectively implemented to develop operational efficiencies and

improve guest satisfaction. This qualitative research contributed to the academic debate within hospitality IT management and the practical implications relevant to the industry.

Table 1. Participants Backgrounds.

Code	Age	Gender	Job Experiences
IT 1	35	Male	10 Years
IT 2	38	Male	5 Years

Data collection was through in-depth interviews. The interviewer has used such interviewing to capture subjective data from each participant. A qualitative methodology provides an advanced exploration of participant experiences, perceptions, and beliefs of the issue at hand, hence, a more advanced understanding of the research issue. Open-ended discussions with participants allow the researcher to obtain detailed narratives that disclose complexity within individual views. It allows participants to state their thoughts openly, and in most cases, such approaches yield insights that quantitative methods could miss. It, therefore, assures the robustness and validity of the research findings.

Data collection in this research was done through interviews by the investigator. He applied the semi-structured approach in the interviews, which should have been less controlling for the participants to respond to questions (Adams, 2015). This method provides a delicate balance: guiding yet giving more latitude for discussion on topics that concern the subject matter. Semi-structured interviews have the added advantage of allowing participants to express and describe their experiences in an almost natural style while still ensuring coverage of themes and objectives considered necessary by the researcher. This way, the researcher drowned out rich qualitative data that revealed subtle variations in perspective among participants. This deepens the level of understanding concerning the subject matter and creates a more interactive and engaging discourse between the researcher and participants, adding to the research findings' validity and reliability. In this regard, the interview design has been carefully considered so that the insights obtained from the interviews provided comprehensive information to enable overall analysis and interpretation of data collected in this study.

The researcher devised an interview guide to facilitate the process during the interviewing of participants. The researcher used a digital meeting platform, Google Meet, for the interviews. The rationale for such a methodological position is to ensure that participants can engage in the interview process in ways not hindered by physical place or time (Thunberg & Arnell, 2022). Because of this, the researcher's digital platform brought forth more inclusive surroundings that can help influence participation from various individuals. Technology here helped not only in making interviews easier but also helped the participants feel comfortable and relaxed, leading to more profound data collection. That means that the researcher fills the gap in possible accessibility and, through this process, understands the research theme.

In this study, the researcher used Indonesian as the medium of communication during the interview. In this case, it would be easier for the participants to provide information quickly and not struggle with barriers in communication. Using the language familiar to participants, they are expected to communicate more effectively and express profound insights into perspectives and experiences. Data collection involved the interview of each participant for a period of between 30 to 60 minutes. It was presumed that the time stipulated was long enough to ensure that the information collected would be complete and reliable enough to bring out a comprehensive understanding of the perspectives and experiences of the participants.

Table 2. Interview guideline

No	Interviews' Questions
1	How did the ransomware attack affect the staff's stress and mental state, but most importantly, the ones directly involved? What emotions do the employees normally express relating to a cyberattack threat-for example, anxiety, fear, or distress?
2	In your view, to what extent was the actual ransomware attack a factor in employee self-efficacy and confidence in managing the cyber threat? Were skill levels enhanced accordingly and their state of preparedness appropriately adapted?
3	How would you describe any changes in employees' attitudes and motivation about cybersecurity training programs before and after the ransomware attack?
4	What would you recommend as strategies an organization could use to factor in aspects of cyber psychology and build a genuinely resilient workforce against such emerging cyber threats?
5	Generally, what can hotels do to enhance cyber-psychological resilience within an individual and group level so that they are better equipped to face any future cyber-attacks? What is the role of communication, leadership response, and employee wellness programs during and after the incident?

In this study, the researcher used Indonesian as the medium of communication during the interview. In this case, it would be easier for the participants to provide information quickly and not struggle with barriers in communication. Using the language familiar to participants, they are expected to communicate more effectively and express profound insights into perspectives and experiences. Data collection involved the interview of each participant for a period of between 30 to 60 minutes. It was presumed that the time stipulated was long enough to ensure that the information collected would be complete and reliable enough to bring out a comprehensive understanding of the perspectives and experiences of the participants.

Thematic analysis was conducted on the data obtained, which included transcription, coding, theme identification, and interpretation. Thematic analysis is an important and flexible method for identifying, analyzing, and reporting patterns or themes within qualitative data (Guest et al., 2014). It helps the researcher establish a total understanding of the aspect under research study. The first step is transcription, whereby the recorded interviews and discussions in focus groups are transcribed to capture all verbal information accurately for analysis. The coding phase followed transcription, where significant data segments will be categorized into meaningful units. It allows for identifying the repeated pattern or theme that cuts across the dataset. After coding, overall themes are then systematically developed. The themes signify the main ideas expressed from the data and reflect insight into the perspectives and experiences of the participants. The last step is interpretation, whereby the identified themes must be placed in context within the broader frame of available literature and research.

RESULT

Three primary themes emerged from the interview findings. These themes provide significant insight into the core areas of interest identified during the research.

Impact on employees mental well-being

The interviews indicated profound psychological aftereffects from the ransomware attack. The IT employees involved in incident management worked harder than usual because their extra efforts were needed to repair and prevent customer data breaches. Their constant fear of repeated system compromises heightened mental distress. Many of them felt overwhelmed by the broad aspect of the attack and unable to put up with the pressures applied to them. The mental impact was even broader

than the direct pressure, hence making the victim's lives deteriorate. Research among cybersecurity professionals reveals that it is pretty standard for them to suffer from burnout, anxiety disorders, or even post-traumatic stress in case of significant security breaches. Given that the attack was overwhelming, it brought physical exhaustion and long-lasting emotional or cognitive effects. The psychological burden exerted on the IT staff during the incident will also have longer-term effects on performance, health, and work commitment. This may lead to a higher risk of low productivity and job satisfaction. It is, therefore, important to note that employees' psychological needs must be considered following such accidents to recover and avoid the long-term effects.

Apart from those personnel directly involved in IT functions, even staff who were always used to non-technical, customer-contact jobs, such as receptionists and customer service representatives, felt increased stress and anxiety. These personnel were hugely hindered in carrying out their duties effectively because of the prolonged disruptions brought about by the ransomware situation. The inability to access reservation platforms and other key systems resulted in delays in responding to customer inquiries and stoked feelings of frustration and helplessness. Such operational inefficiency implicated not only the workflow but also self-confidence and perceived self-efficacy. This meant that many of them could not work and perform their duties as usual. This stress was catalyzed by the fact that they were highly dependent on digital systems, meaning their jobs were very vulnerable in case of technological disruptions. This incident also shows how important it is to ensure that powerful cyber defense mechanisms occur at all levels within the organization's sectors since operational disruption goes beyond IT personnel to affect the organization's overall efficiency and employee well-being. In this respect, it is recommended that crisis management training should be extended to all staff in the direction of minimizing anxiety and maintaining productivity in these cases.

This entire infiltration period and subsequent remediation after the ransomware attack were a period of great uncertainty and stress among the staff, especially those directly involved in the mitigation efforts at the front line. As would logically be expected, interviews reveal that the psychological impact on such persons was relatively high, with many reporting significant depletion of emotional and mental resiliency. While the incident tested the organization's technical competence and business continuity plans, the cost to individual welfare was not insignificant. This further raises the crucial importance of mental health support and counseling services in post-incident recovery strategies, particularly for staff involved in high-risk cybersecurity interventions. More significant organizational effects of such an incident go beyond the initial pure technical challenges and point to the omission in most business continuity frameworks, which often neglect the human dimension when cybersecurity incidents occur. If these psychological effects are not treated promptly and efficiently, they may lead to burnout, a lowering of job satisfaction, and even long-term mental health consequences. Hence, post-cyberattack recovery needs to be holistic, balancing technical remediation with psychological support of employees to ensure workforce resilience and organizational well-being post-incident.

There is an increasing awareness in management that the human factor in cybersecurity deserves more attention. Besides the needed technical capabilities, the capability of building both individual and organizational cyberpsychology resilience must be developed. This is all the more important in light of the psychological burden that employees are under when cyber-attacks breach existing security systems. Besides the purely technical challenges, staff involved in responding to these kinds of incidents are very often exposed to unusually high levels of emotional and mental pressure, possibly with long-term effects such as burnout, anxiety, or post-traumatic stress. Therefore, every organization should consider enhancing cybersecurity competencies among their staff and protecting their mental health. Programs involving mental wellness, adequate support systems, and an open

environment to share mental health problems can help build resilience within the workforce. The holistic approach towards cybersecurity management encompasses the importance of psychological well-being in achieving a strong defense posture for better mitigating cyber threats and organizational security outcomes.

Effects on attitudes towards cybersecurity training

The interviews' findings provided that the cybersecurity training among hotel employees was not emphasized prior to the ransomware attack. This is regarded as less significant on the part of the hotel compared to other activities. This attitude could be translated into a lack of caution in adhering to best practices and security protocols over time at both the individual and organizational levels. It probably created lapses in the mechanisms of defense that an organization builds against newly emerging threats due to inconsistency in engendering the culture of cybersecurity preparedness. Without a robust security awareness culture, the employees would have taken digital risk mitigation as an unduly insignificant concern and were not vigilant enough in safeguarding sensitive information. The organizational priority appeared to tilt more toward the immediate business concerns at the expense of the long-term consequences of poor cybersecurity mechanisms. This incident thus marks a common trend across industries, whereby cybersecurity comes out as the last priority until some significant breach points out the need for stronger prevention measures. In this respect, the attack emphasized incorporating all-round cybersecurity training into an operational core strategy to avoid such weaknesses in the future.

This ransomware intrusion was a watershed moment in the organization's life since it illuminated the operational framework's vulnerabilities. It also made them realize how important continuous professional development and training for all staff members and engendered a culture of learning within the company. There was a sea change in the organizational approach toward training, a key ingredient in securing the company's long-term survival. With continued empathy from the employees, the feeling of their collective responsibility for customer data protection and service functionality integrity keeps growing. The transformation shows that cybersecurity has to be done proactively, with full training, to enhance the competencies of individuals and eventually make the organization resilient against present and future threats. This finally catalyzed a better-informed workforce that is more competent in overcoming all the complications and obstacles regarding cybersecurity challenges in an ever-growing digital world.

Indeed, the shift in attitude became evident through heightened participation in newly initiated training programs for the hotel management following the incident. As demonstrated, managers stated that attendance and participation in the training sessions were higher than in previous programs. This suggests a positive leaning toward the development of employees and the organization's growth. However, both managers were concerned that this heightened motivation would eventually level off if constant reminders of the training results were not given. If management wants the motivations to be longer-lasting, open communication about how the training is implemented and its benefits should be established to engender a culture of continuous improvement. Besides, feedback mechanisms might be included to further develop the relevance of training programs so that employees can be more interested in their personal and professional development.

The ever-changing dynamics of the cyber landscape require regular messaging to enable employees to change their attitudes towards cybersecurity. The personnel should be made aware of new threats, coupled with the evolution of their perception of cybersecurity dynamics. This will help instill a culture of continuous learning that leads to better organizational resilience in the long term.

The complacency that perhaps preceded a breach in security has to be outworked to prevent regression. Proactive and continuous reinforcement of the importance of cybersecurity training remains paramount. Indeed, a ransomware attack was a catalyst in shifting perspectives among employees. Refresher training, however, inconsistent intervals are paramount regarding emerging risks and respective roles played by employees in mitigating risks. Such an approach would retain the changed mindset and build shared commitment toward sound cybersecurity practices to ensure an improved organizational culture. Besides, embedding periodic evaluation and feedback mechanisms within the training can facilitate an adaptive learning environment. In such an environment, employees become inclined to proactively tackle emergent threats to solidify the organization's defenses against cyber threats. This makes employees feel a part of the responsibility in one way or another, closer to the overall security, playing an active rather than passive role in mitigating those cyber risks. The final piece in this complex jigsaw puzzle that each business must be to navigate the modern cyber threat landscape and stay secure and in business for years to come is a well-informed and vigilant workforce.

Strategies for building cyber resilience

Lessons learned from the ransomware incident show that regular cyber awareness campaigns are important in making organizations resilient. As both IT managers outlined, a vigilance culture is important to avoid complacency since the threat landscape continuously changes. Regular refresher sessions are put in place to inculcate the culture of preparedness and are also applied even when there is inevitable turnover within an organization. They also pointed out that such training should be individualized, based on a particular role, and must consider the various human factors in an organization. One-size-fits-all training does not work; instead, content must be prepared according to the needs and requirements of the specific role of individuals to make the material more relevant and allow better retention by establishing role-specific learning pathways. Besides, understanding human psychology in training materials design and delivery significantly enhances the educational impact because it teaches the process to learners' cognitive and emotional characteristics. Through such strategies, organizations will be able to develop a workforce aware of the threats and prepared to respond effectively to minimize risks emanating from these emerging cyber threats.

One key approach to reinforcing this organizational resilience would involve constructing cyber response plans that detail roles and responsibilities and expert knowledge. Drawing the lines clearly like this will prevent confusion about who does what in response to cybersecurity incidents, engendering confidence among the staff and supporting effective mitigation. Counseling support and discussion groups are vital here, merging technical and psychological standpoints on resilience. The measures would, of course, be integral to strong leadership impetus. Senior management overtly prioritizes cybersecurity, which sets an inspired and watchful tone within the organization. Well-defined policies disseminated, strategic investments in security infrastructure, and acknowledgment of staff training initiatives help set an appropriate "tone from the top." Moreover, the accessibility to management to listen to and handle employee issues cements organizational commitment towards cybersecurity and empowers the staff to make them resilient. In this respect, the openness in communication and collaboration will enhance organizational adaptive capacity against evolving cyber threats. Together, these elements create a robust framework that allows both individual and collective responses to cyber incidents that may affect the integrity of an organization and operational continuity.

In a nutshell, interviewees call for comprehensive mechanisms encompassing frequent skill development, role-specific knowledge, standardized response mechanisms, psychological counseling, and vocal leadership commitment in the interest of resilience. This will undoubtedly contribute to all-

round development within the organization and also serve to overcome the complexities of workforce resilience. Integrating technological safeguards with human-centered factors would help organizations fortify their workforce against the complexities of emerging cyber threats. The synthesis of such skills, knowledge, and support structures assists the staff in preparing to deal with that rapidly changing cyber landscape. Moreover, a culture of continuous learning and adaptability will significantly enhance the organization's responsiveness to unexpected challenges, culminating in sustainable operational efficacy and resilience that creates a sound mechanism for responding to the risks that have been assessed.

DISCUSSION

One of the key findings of the research is that ransomware incidents significantly impact the psychological condition and mental well-being of personnel, especially those directly engaged in incident response. This is consistent with the extant literature, in which cybersecurity professionals are disproportionately prone to burnout, anxiety, and PTSD caused by extreme pressures associated with serious security breaches (Sachs et al., 2022). This research contributes further empirical evidence to this debate but, at the same time, narrows it down to hotel staff in Indonesia. The paper has highlighted the critical need to consider the human factor in cybersecurity management. In this regard, adequate support mechanisms should be introduced to protect employees' well-being during and after such traumatic events (Brooks, Rubin et al., 2019). Embedding mental health resources and training programs that foster resilience may be critical in mitigating the psychological impact of ransomware attacks. By creating a culture of psychological safety and support, organizations were in a better position to improve general mental health among their staff and enhance the capability of responding effectively to possible cybersecurity threats (Brooks, Dunn et al., 2019).

Indeed, the study depicts a dramatic change in attitude toward cybersecurity training, considered a low priority before the incident but now perceived as indispensable. This confirms the literature that most organizations only take measures to protect against cyber-attacks after an incident has occurred (Li & Liu, 2021). A real strength of this research is that it has depicted the positive evolution of perspectives that may emerge in a learning experience related to cybersecurity. However, long-term motivation to continue training has always posed a great challenge for organizations. In this respect, future research could still be devoted to testing diverse methodologies and communication methods supporting sustained engagement and reinforcement over time. Furthermore, it would be gratifying to delve deeper into the role organizational culture and leadership support can play in creating a proactive cybersecurity stance. Awareness will only be high, and the cybersecurity setup of organizations will be resilient through well-structured and adaptive training that considers the ever-changing face of cyber threats.

The recommendations of strategies for building resilience support technical and human factors, again aligning with the concept of cyber psychological resilience as defined by Matveev et al. (2021). Specialized and periodic training combined with strong leadership support and a well-supported wellness program lays a sound foundation for an organizational security culture. Furthermore, it must be recognized that even though this could provide a good foundation, further steps in providing standardized frameworks would take more work. Thus, the subsequent efforts should be geared towards practical empirical verifications of the effectiveness of the proposed frameworks to achieve pragmatic viability and enhance overall resilience in cybersecurity contexts (Taylor & Whitty, 2024). The evaluation validates the proposed strategies and draws on best practices that can be disseminated across a wide array of sectors toward enhanced resilience in cybersecurity posture.

Key findings from the case study reveal significant implications for organizational cyber-resilience development in an Indonesian hospitality context. Despite its small-scale research, it reinforces the contribution of existing literature and points out some essential psychological and cultural factors commonly ignored in cybersecurity discussions. These dimensions combined provide a better understanding of the challenges of building resilience against threats emanating from cyberspace. This requires longitudinal research and monitoring of prescribed interventions to redefine future cybersecurity strategies and policies. Such an investigation provides practitioners and policy-makers with an integrated framework to develop a more assertive cybersecurity posture for the hospitality industry. Further, a diversified set of stakeholders could make this development of focused strategies targeting the peculiar vulnerabilities of this industry all the more constructive for improved awareness and, thereby, proactive steps against cyber risks.

CONCLUSION

This case study developed organizational resilience to ransomware attacks in the Indonesian hospitality sector. The study explained some important issues through comprehensive qualitative interviews conducted with the IT managers of two prestigious hotels that had faced ransomware incidents: the ransomware attack may affect employees' psychology and mental health, especially those working as an incident response team. It also had a positive impact on the attitudes of staff toward cybersecurity training, underlying the embedding of a proactive security culture. Long-term motivation cannot be achieved without regular reinforcement and highlighting of cybersecurity practices. The study has specified several strategies to promote resilience, including technical measures and human factors: specialized training, pre-defined response plans, strong leadership support, and mental health initiatives. These multilevel strategies have their place in developing the security framework that mitigates cyber threats without compromising the well-being of employees. While these findings have some practical preliminary conclusions, further longitudinal research with various stakeholders is needed. This would rigorously assess the proposed frameworks for their effectiveness in enhancing security culture while ensuring the workforce's long-term well-being. In addition to the above, there will be a need to understand the changing nature of cyber threats and the adaptive methods the organizations need to take to be resilient in the dynamically developing threat environment.

DECLARATION

Acknowledgment

I hereby extend my heartfelt appreciation to all those who contributed to completing this research, "Cyber Resilience in Combating Ransomware Attacks: A Psychological Case Study Perspective on the Hospitality Industry." First and foremost, I would like to thank my academic advisor for his valuable guidance, support, and expertise throughout this research process. Your insights and encouragement have been crucial in shaping my understanding of such complexities as cyber resilience and their psychological implications within the hospitality sector.

I would also like to thank the hospitality professionals who participated in this study by sharing their experiences and views on ransomware attacks. Through the sharing of your experiences and views, your openness to insights and informative discussions has enriched this research. Thanks to my colleagues and peers for their support and constructive criticism. Our research group's collaborative spirit fosters a stimulating inquiry and growth environment. I am also thankful for the family and friends who have been supportive and understanding. Believing in me, you pushed me through obstacles and enabled me to work for excellence.

Thanks to all for being part of this important work.

Author contribution statement

The lead researcher in this study is Author 1, who led the general design and planning of the research. They went through an extensive literature review to identify the gaps in prior research and formulated overall research questions used in this study. Author 1 selected the appropriate methodologies, designed the instruments for data collection, and took the lead in recruiting participants while ensuring standards of ethics were upheld. They considered the data very carefully, interpreting the findings in light of the theoretical framework established. While preparing the manuscript, Author 1 wrote the introduction, methodology, results, and discussion sections, keeping the journal guidelines in mind. Author 2, the co-researcher, played a vital role in supporting the research process given the literature review and helping develop research instruments. Interviews through data collection, responses, and participation in the preliminary data analysis supported the study. Besides that, Author 2 contributed by providing critical comments during the writing of the manuscript, hence revising and enhancing clarity and coherence in the final article. In this way, their joint contribution empowered the research results and made the quality of the manuscript even higher.

Funding statement

This research did not receive any specific grant from funding agencies in the public, commercial, or nonprofit sectors.

Data access statement

The data described in this article are openly available in Google Scholar, Chicago, and ERIC.

Declaration of interest's statement

The authors declare no conflict of interest.

Additional information

No additional information is available for this paper.

REFERENCES

Adams, W. C. (2015). Conducting Semi-Structured Interviews. In E. N. Kathryn, P. H. Harry, & S. W. Joseph (Eds.), *Handbook of practical program evaluation*, 492–505. https://doi.org/10.1002/9781119171386.ch19

Al-rimy, B. A. S., Maarof, M. A., & Shaid, S. Z. M. (2018). Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. *Computers and Security 74*, 144–166). https://doi.org/10.1016/j.cose.2018.01.001

Alawida, M., Omolara, A. E., Abiodun, O. I., & Al-Rajab, M. (2022). A deeper look into cybersecurity issues in the wake of Covid-19: A survey. *In Journal of King Saud University - Computer and Information Sciences 34(10)*, 8176–8206. https://doi.org/10.1016/j.jksuci.2022.08.003

Appiah, G., Amankwah-Amoah, J., & Liu, Y. L. (2022). Organizational architecture, resilience, and cyberattacks. *IEEE Transactions on Engineering Management, 69(5)*, 2218–2233. https://doi.org/10.1109/TEM.2020.3004610

Aqilah, N., Farok, Z., & Zolkipli, M. F. (2024). Incident response planning and procedures. *In Borneo International Journal*, *7(2)*. www.majmuah.com

Braun, V., Clarke, V., Braun, V., & Clarke, V. (2017). Applied qualitative research in psychology. *Applied Qualitative Research in Psychology, 0887*(2006). https://doi.org/10.1057/978-1-137-35913-1

Brooks, S. K., Dunn, R., Amlôt, R., Rubin, G. J., & Greenberg, N. (2019). Protecting the psychological wellbeing of staff exposed to disaster or emergency at work: A qualitative study. *BMC Psychology, 7(1).* https://doi.org/10.1186/s40359-019-0360-6

Brooks, S. K., Rubin, G. J., & Greenberg, N. (2019). Traumatic stress within disaster-exposed occupations: Overview of the literature and suggestions for the management of traumatic stress in the workplace. In British Medical Bulletin, 129(1), 35–51). https://doi.org/10.1093/bmb/ldy040

Cartwright, E., Hernandez Castro, J., & Cartwright, A. (2019). To pay or not: Game theoretic models of ransomware. *Journal of Cybersecurity, 5(1).* https://doi.org/10.1093/cybsec/tyz009

Clarke, R. V. G. (1980). Situational crime prevention: Theory and practice. *The British Journal of Criminology, 20(2)*, 136–147. https://doi.org/10.1093/oxfordjournals.bjc.a047153

Cobanoglu, C., Dogan, S., Berezina, K., & Collins, G. (2021). Hospitality and tourism information technology. *University of South Florida M3 Publishing, 17*. https://doi.org/10.5038/9781732127593

Connolly, L. Y., Wall, D. S., Lang, M., & Oddson, B. (2020). An empirical study of ransomware attacks on organizations: An assessment of severity and salient factors affecting vulnerability. *Journal of Cybersecurity, 6(1)*. https://doi.org/10.1093/CYBSEC/TYAA023

Ell, M. (2024, April 9). *Cyber security breaches survey 2024*. United Kingdom Government.

Florido-Benítez, L. (2024). Cybersecurity is applied by online travel agencies and hotels to protect users' private data in smart cities. *Smart Cities, 7(1),* 475–495. https://doi.org/10.3390/smartcities7010019

Guest, G., MacQueen, K., & Namey, E. (2014). Introduction to applied thematic analysis. *SAGE Publications*, 3–20. https://doi.org/10.4135/9781483384436

Gundu, T., & Mmango, N. (2024). A cybersecurity collaborative model: best practices sharing among south african tourism and hospitality businesses. *Proceedings of the 7th International Conference on Tourism Research, 7(1)*, 222–231. https://doi.org/10.34190/ictr.7.1.2159

He, Z., Huang, H., Choi, H., & Bilgihan, A. (2023). Building organizational resilience with digital transformation. *Journal of Service Management, 34(1)*, 147–171. https://doi.org/10.1108/JOSM-06-2021-0216

Law, R., Leung, D., Au, N., & Lee, H. A. (2013). Progress and development of information technology in the hospitality industry: evidence from cornell hospitality quarterly. *Cornell Hospitality Quarterly, 54(1)*, 10–24. https://doi.org/10.1177/1938965512453199

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports, 7*, 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126

Marcucci, G., Antomarioni, S., Ciarapica, F. E., & Bevilacqua, M. (2022). The impact of operations and it-related industry 4.0 key technologies on organizational resilience. *Production Planning and Control, 33(15)*, 1417–1431. https://doi.org/10.1080/09537287.2021.1874702

Matveev, V., Olena Eduardivna, N., Stefanova, N., Khrypko, S., Ishchuk, A., Ishchuk, O., & Bondar, T. (2021). Cybercrime in the economic space: Psychological motivation and semantic-terminological specifics. *IJCSNS International Journal of Computer Science and Network Security, 21(11)*. https://doi.org/10.22937/IJCSNS.2021.21.11.18

Sachs, J. D., De Neve, J.-E., Helliwell, J. F., Aknin, L. B., Layard, R., Iyengar, R., Karadag, O., Wang, S., & Quintarelli, S. (2022). *Global happiness and well-being policy report global council for happiness and well-being.* Happiness Council. https://www.happinesscouncil.org/

Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking cyber threats: A framework for the future of cybersecurity. *Sustainability (Switzerland), 15(18)*. https://doi.org/10.3390/su151813369

Taylor, J., & Whitty, M. (2024). An exploration of the awareness and attitudes of psychology students regarding their psychological literacy for working in the cybersecurity industry. *Psychology Learning and Teaching, 23(2)*, 298–314. https://doi.org/10.1177/14757257231214612

Thunberg, S., & Arnell, L. (2022). Pioneering the use of technologies in qualitative research–A research review of the use of digital interviews. *International Journal of Social Research Methodology, 25(6)*, 757–768. https://doi.org/10.1080/13645579.2021.1935565

Vogus, T. J., & Sutcliffe, K. M. (2007). Organizational resilience: Towards a theory and research agenda. *IEEE, 8(7)*, 3418–3422. http://doi.org/10.1109/ICSMC.2007.4414160

Wirza, Y. (2018). A narrative case study of Indonesian EFL learners' identities. *Indonesian Journal of Applied Linguistics, 8(2)*, 473–481. https://doi.org/10.17509/ijal.v8i2.13313

Yanuarni, E., Iqbal, M., Astuti, E. S., Mawardi, M. K., & Alfisyahr, R. (2024). Determinants of business recovery: The role of government support as moderator (a study on tourism SMEs affected by Lombok earthquake, Indonesia). *Human Systems Management, 43(1)*, 79–97. https://doi.org/10.3233/HSM-220171