EVALUATING CYBERSECURITY PREPAREDNESS IN SMALL BUSINESSES: A STUDY OF SECURITY MEASURES, EMPLOYEE AWARENESS, AND THREAT PREVENTION

[1]Kulkarni Pranjal Suryakant, [2]Dr. Pramod Kumar
[1]Research Scholar, [2]Supervisor
[1-2]Glocal School of Computer Science, The Glocal University, Distt. Mirzapur, Saharanpur (U.P.), India

Abstract
This study examines cybersecurity preparedness in small businesses with a focus on security measures, employee awareness, and threat prevention practices. In the digital business environment, small enterprises increasingly rely on information systems, online transactions, cloud services, and electronic communication, which makes preparedness for cyber threats highly important. The study highlights the meaning of cybersecurity preparedness as the ability of a business to prevent, detect, and respond to cyber risks effectively. It reviews key security measures such as network security, endpoint protection, backup and recovery systems, and authentication controls. The paper also emphasizes the role of employee awareness, cyber hygiene, and training in reducing human error and improving security behavior. In addition, it discusses threat prevention practices such as identifying phishing attempts, monitoring unusual activities, and promoting safe digital practices. The study concludes that cybersecurity preparedness is essential for small businesses to strengthen resilience, reduce vulnerability, and ensure secure and sustainable operations.

Keywords
Cybersecurity Preparedness, Small Businesses, Security Measures, Employee Awareness, Threat Prevention, Cyber Hygiene, Organizational Resilience, Information Security

1. Introduction

Cybersecurity preparedness in small businesses refers to the ability of an organization to anticipate, prevent, detect, and respond effectively to cyber threats through appropriate security measures, employee awareness, and threat prevention practices. In the modern digital environment, small businesses increasingly rely on online transactions, cloud services, digital communication, business software, and connected systems, which makes preparedness essential for protecting operations, customer information, and financial data. Cybersecurity preparedness is important because small businesses often face growing cyber risks while operating with limited resources, less technical support, and weaker security structures than larger organizations. The problem is that many small businesses remain insufficiently prepared due to gaps in network security, endpoint protection, backup and recovery systems, authentication controls, employee training, and monitoring practices. In this context, the present study examines cybersecurity preparedness in small businesses by focusing on security measures, employee awareness, threat prevention practices, and the organizational factors that influence their overall readiness against cyber threats.

2. Cybersecurity Preparedness: A Theoretical Overview

Cybersecurity preparedness refers to the extent to which an organization is capable of anticipating, preventing, identifying, responding to, and recovering from cyber threats that may affect its digital assets, systems, and business functions. In the context of small businesses, preparedness is not limited to the existence of technical security tools; rather, it reflects the overall readiness of the organization to deal with cyber risks through planning, awareness, controls, and coordinated action. It involves a proactive state in which the business understands its vulnerabilities, knows what assets are critical, and adopts measures to reduce exposure before an attack occurs. This concept is especially important in small business environments because digital dependence has increased significantly, while security maturity often remains low. Corallo et al. (2020) explained that critical digital assets and business impacts are closely linked, meaning that the failure to protect core systems can directly affect organizational performance and continuity.

The concept of preparedness is closely connected with security readiness. Security readiness means the degree to which a business has the structures, practices, and capabilities needed to manage cyber risks effectively. This includes technical readiness, such as secure systems and access controls, and organizational readiness, such as policies, employee compliance, and leadership involvement. For small businesses, security readiness often determines whether cyber incidents remain manageable disruptions or develop into serious crises. Tu et al. (2018) showed that cybersecurity risk management in small and medium-sized enterprises depends heavily on how organizations perceive risks and organize their response capacity. A prepared business is therefore one that not only installs defensive tools

but also develops a mindset of continuous vigilance and adaptation.

Preparedness is also strongly related to organizational resilience. Organizational resilience refers to the ability of a business to continue functioning, recover quickly, and maintain stability when facing disruption. In cybersecurity, resilience means that even if an incident occurs, the business is able to minimize damage, protect essential operations, restore systems, and maintain stakeholder trust. Small businesses are particularly vulnerable because they often lack specialized recovery teams, formal incident response plans, and financial buffers. For this reason, preparedness becomes a foundation of resilience. A business that is better prepared is more likely to absorb cyber shocks and recover with less damage than one that reacts only after problems arise. Parker and Gidley (2021) emphasized that small business cybersecurity must be understood not only in terms of threats but also in terms of future-oriented readiness and strategic response capacity.

Another theoretical dimension of cybersecurity preparedness is the role of prevention in cyber defense. Prevention is one of the most important aspects of effective cybersecurity because it seeks to reduce the likelihood of incidents before they occur. Preventive cybersecurity includes measures such as secure configurations, regular updates, awareness training, authentication controls, safe user practices, and continuous monitoring. In small businesses, prevention is especially valuable because these organizations often do not have the capacity to absorb the consequences of major cyber incidents. Hina and Dominic (2018) argued that policy compliance is central to information security in SMEs, suggesting that prevention depends not only on technical tools but also on behavioral discipline and organizational commitment. Thus, the theoretical understanding of preparedness highlights that cybersecurity is not merely reactive defense; it is a structured and preventive condition of readiness that supports resilience, continuity, and long-term organizational security.

3. Security Measures Adopted by Small Businesses

Small businesses adopt various security measures to protect their digital infrastructure, though the strength and consistency of these measures differ widely across organizations. One of the most important areas is network security, which involves protecting internal networks, internet connections, Wi-Fi systems, and communication channels from unauthorized access and intrusion. Network security measures may include firewalls, secure routers, network segmentation, virtual private networks, and intrusion detection tools. For small businesses, network security is essential because daily operations often depend on internet-connected systems such as cloud platforms, billing software, customer databases, and communication tools. If network protection is weak, attackers may gain access to multiple business functions at once. Corallo et al. (2020) highlighted that business-critical assets are often interconnected, which means that a compromised network can have broad operational consequences.

Endpoint protection is another major security measure used in small businesses. Endpoints include laptops, desktops, smartphones, tablets, and other devices connected to the business network. These devices are frequent targets of malware, ransomware, spyware, and unauthorized access attempts. Endpoint protection usually includes antivirus software, anti-malware tools, device encryption, secure configurations, and regular software patching. Since employees in small businesses may use multiple devices for communication and work tasks, endpoint protection becomes essential for reducing risk at the user level. Pratt and Goundar (2021) noted that security measures in SMEs, especially in cloud-based working environments, depend heavily on how well endpoints are protected and how aware employees are of security responsibilities.

Backup and recovery systems are also central to small business cybersecurity. Backups help businesses restore essential files, records, and systems after ransomware attacks, accidental deletion, hardware failure, or other disruptions. Recovery systems ensure that business operations can resume with minimal delay after a cyber incident. In small businesses, this is especially important because operational interruptions can quickly affect revenue, customer service, and trust. A reliable backup strategy may include cloud backups, offline backups, scheduled recovery points, and testing of restoration procedures. Without effective backup and recovery measures, even a single cyberattack can create long-term damage. Tu et al. (2018) indicated that SME risk management requires not only risk recognition but also operational recovery mechanisms, which makes backups a vital part of preparedness.

Authentication systems are another key security measure. Authentication refers to the methods used to verify the identity of users before granting access to systems, accounts, or data. Traditional password-based access remains common in small businesses, but stronger measures such as multi-factor authentication, one-time verification codes, biometric checks, and access-role controls are increasingly necessary. Authentication systems reduce the likelihood of unauthorized access, especially when passwords are weak, stolen, or reused across platforms. Strong authentication is particularly important for protecting email accounts, cloud services, payment systems, and administrative platforms. However, many small businesses still rely on simple credential practices due to convenience or lack of technical guidance. This makes authentication both a technical and managerial issue. Effective security measures in small businesses therefore depend not only on the availability of tools but also on whether these measures are properly maintained, consistently used, and supported by broader organizational awareness.

4. Employee Awareness and Cybersecurity Behavior

Employee awareness is one of the most important dimensions of cybersecurity preparedness because employees are often the first point of interaction with cyber threats. No matter how advanced technical controls may be, security can be weakened if employees fail to identify suspicious behavior, ignore safe practices, or make careless decisions in daily digital activities. In small businesses, employee awareness is particularly significant because formal cybersecurity departments are often absent and staff members usually perform multiple roles. This means that ordinary employees are not only users of systems but also practical defenders of business data and digital resources. Bada and Nurse (2020) argued that developing a cybersecurity awareness culture is essential for organizations because security failures often arise from resistance, low engagement, and insufficient behavioral integration. In small businesses, where informal work patterns are common, awareness becomes even more critical.

Human error remains one of the leading causes of cybersecurity incidents. Employees may click malicious links, open unsafe attachments, use weak passwords, share credentials, ignore update notifications, or access business systems through insecure networks. Such errors do not always result from carelessness alone; they may also arise from lack of knowledge, time pressure, poor policy communication, or misunderstanding of risk. Zwilling et al. (2020) showed that cybersecurity awareness, knowledge, and behavior are closely related, indicating that people who better understand cyber risks are more likely to behave securely. This relationship is highly relevant in small businesses, where even one employee mistake may expose sensitive customer information, interrupt operations, or allow attackers into the wider system. Therefore, cybersecurity behavior must be understood as a practical outcome of awareness, knowledge, and workplace culture.

Cyber hygiene and training are necessary for improving employee behavior and reducing preventable incidents. Cyber hygiene refers to the routine practices that help maintain digital safety, such as using strong passwords, updating software, avoiding suspicious websites, checking email authenticity, locking devices, and following secure file-sharing procedures. These practices must become part of everyday work habits rather than occasional reminders. Training helps employees understand current threats and teaches them how to respond properly in real situations. It also creates consistency in behavior across the organization. Hina and Dominic (2018) emphasized that compliance with information security policies is central to organizational protection, while Bada and Nurse (2020) showed that awareness culture must be actively developed rather than assumed. In small businesses, where informal communication often replaces formal systems, training and cyber hygiene are necessary to convert awareness into reliable security behavior.

5. Threat Prevention Practices

Threat prevention practices are the proactive activities through which small businesses attempt to reduce the likelihood of cyber incidents before damage occurs. One of the most important prevention practices is identifying suspicious emails and phishing attempts. Phishing remains one of the most common methods used by cybercriminals to gain access to passwords, financial details, and system credentials. Employees may receive emails that appear legitimate but contain deceptive links, harmful attachments, or urgent requests for sensitive information. Because phishing often targets human judgment rather than technical weaknesses, prevention depends heavily on awareness, verification habits, and caution in communication. Bada and Nurse (2020) noted that awareness culture is central to resisting social engineering threats, while Zwilling et al. (2020) linked secure behavior directly to cybersecurity knowledge and understanding.

Monitoring unusual activities is another important threat prevention practice. This includes observing unexpected login attempts, unusual file access, unexplained system slowdowns, suspicious account behavior, or irregular network traffic. In small businesses, monitoring may not always involve advanced security operation centers, but even basic observation, alerts, and review practices can help identify early warning signs. For example, repeated failed logins, sudden file changes, or unauthorized account usage may indicate ongoing compromise. Prevention becomes more effective when businesses do not wait for a major incident but pay attention to minor irregularities that may signal deeper threats.

Safe browsing and download practices are also essential to threat prevention. Employees frequently interact with online resources, websites, files, and software tools as part of daily operations. If they download unverified software, open files from unknown sources, or browse insecure websites, they increase the risk of malware infection and unauthorized access. For this reason, threat prevention must include clear guidance on how to use the internet safely, which sources to trust, and how to verify digital content before interacting with it. Pratt and Goundar (2021) indicated that security in SMEs is closely tied to employee practices, especially in technology-enabled environments where user actions can create or reduce risk.

Preventive controls and monitoring systems support these practices at the technical level. These may include email filtering, antivirus systems, firewall rules, device monitoring, access restrictions, software patch management, and authentication controls. Such measures create barriers that reduce the chances of threat entry and spread. However,

prevention is most effective when technical controls are combined with human vigilance. Threat prevention in small businesses therefore requires both everyday caution and supportive systems. It is not a one-time activity but a continuous discipline that combines awareness, observation, safe behavior, and basic technical defense.

6. Factors Affecting Cybersecurity Preparedness

Cybersecurity preparedness in small businesses is influenced by several organizational and operational factors. One important factor is business size. Smaller firms often have fewer employees, lower budgets, and limited access to specialized expertise, all of which can reduce their preparedness level. They may depend on general-purpose software, informal practices, and outsourced technical support rather than structured internal security systems. As a result, they are often less able to implement layered defenses, regular monitoring, and formal incident response processes. Heidt et al. (2019) emphasized that SMEs occupy a distinct position in cybersecurity research because their structural characteristics shape both their vulnerabilities and their response capabilities.

Technology usage is another major factor. Businesses that rely heavily on cloud services, digital payments, online platforms, mobile devices, and remote access systems face a wider and more complex threat surface. The more digital tools a business adopts, the more important preparedness becomes. However, increased technology usage does not automatically produce better security. In many cases, businesses adopt digital tools faster than they develop the controls needed to manage associated risks. Corallo et al. (2020) showed that digital interdependence increases the importance of protecting critical assets, while Pratt and Goundar (2021) highlighted that technology adoption in SMEs requires parallel attention to awareness and security controls.

Management support also plays a decisive role in preparedness. When business leaders treat cybersecurity as a strategic priority, organizations are more likely to invest in protective measures, encourage training, establish policies, and promote compliance. In contrast, when management sees cybersecurity as only a technical or secondary issue, security efforts tend to remain weak, fragmented, or reactive. Leadership influences whether employees take cybersecurity seriously and whether resources are allocated for preparedness. Tu et al. (2018) suggested that risk management in SMEs is deeply shaped by managerial perception and organizational commitment, making leadership support central to readiness.

Cybersecurity culture is another critical factor. Culture refers to the shared attitudes, values, and habits that shape how people behave toward security within the organization. A strong cybersecurity culture encourages caution, accountability, reporting of suspicious events, and respect for security procedures. A weak culture, on the other hand, may normalize shortcuts, password sharing, ignored warnings, and informal access practices. Bada and Nurse (2020) argued that awareness culture is essential for effective cybersecurity, while Hina and Dominic (2018) showed that compliance behavior is strongly affected by organizational context. In small businesses, culture can be especially influential because teams are smaller, informal norms spread quickly, and daily practices are often shaped by leadership example. Thus, preparedness is not determined by technology alone; it is shaped by size, digital dependence, managerial commitment, and the internal culture of security.

Conclusion

In conclusion, cybersecurity preparedness is essential for small businesses because their increasing dependence on digital systems makes them more vulnerable to cyber threats and operational disruption. The study shows that preparedness is shaped by a combination of security measures, employee awareness, and threat prevention practices, all of which work together to strengthen organizational resilience. Measures such as network security, endpoint protection, backup and recovery systems, and authentication controls provide technical protection, while employee awareness, cyber hygiene, and safe digital behavior reduce risks caused by human error. At the same time, factors such as business size, technology usage, management support, and cybersecurity culture significantly influence the overall level of preparedness. Therefore, small businesses must adopt a proactive and balanced approach to cybersecurity in order to reduce vulnerability, protect critical assets, and ensure secure and sustainable business operations.

References

Bada, M., & Nurse, J. R. C. (2020). Developing cybersecurity awareness culture in organisations: A review of current approaches and resistance. *Journal of Cyber Policy, 5*(2), 260–277. https://doi.org/10.1080/23738871.2020.1791424

Corallo, A., Lazoi, M., & Lezzi, M. (2020). Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts. *Computers in Industry, 114*, 103165. https://doi.org/10.1016/j.compind.2019.103165

Heidt, M., Gerlach, J. P., & Buxmann, P. (2019). Investigating the role of small and medium-sized enterprises in cybersecurity: A systematic review of evidence and theoretical perspectives. *The Journal of Strategic Information Systems, 28*(2), 167–191.

Hina, S., & Dominic, P. D. D. (2018). Information security policies' compliance: A perspective of SMEs. *Procedia Computer Science, 124*, 705–712. https://doi.org/10.1016/j.procs.2017.12.208

Lal, B., Dwivedi, Y. K., & Williams, M. D. (2012). Checklists for help-desk agents: A case study of a small enterprise. *Journal of Enterprise Information Management, 25*(2), 150–165.

Parker, C. F., & Gidley, J. M. (2021). Small business cybersecurity: A review of the literature and future research directions. *International Journal of Information Management, 57*, 102283.

Pratt, B., & Goundar, S. (2021). Security measures and employee awareness in small and medium enterprises: A case study of cloud computing adoption. *International Journal of Cloud Applications and Computing, 11*(2), 1–15.

Saba, T., Haseeb, K., Ahmed, I., & Rehman, A. (2020). Secure and energy-efficient framework using Internet of Medical Things for e-healthcare. *Journal of Infection and Public Health, 13*(10), 1567–1575. (Focuses on sector-specific SME security measures).

Tu, Z., Yuan, Y., & Archer, N. (2018). Understanding cybersecurity risk management in small and medium-sized enterprises: A qualitative study. *Journal of Small Business Management, 56*(1), 1–18.

Zwilling, M., Klein, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Kölgeli, H. (2020). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems, 62*(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269