# Mitigating Insider Threats with Advanced Cyber-Security Measures in Nursing Staffing Agencies

Temitope Oyinkansola Asade[1*], Olutoye Ransome-Kuti[1], Ojonoka Erika Atawodi[2], Oyindamola Omolayo[1], Nonye Fortune Lesinwa[1], Tolulope Awe[1]

1. School of Business, Westcliff University, 17877 Von Karman Avenue, 4th floor, Irvine CA 92614, USA
2. Harrisburg University of Science and Technology, 326 Market Street, Harrisburg, PA 1710, USA

*T.Asade.2334@westcliff.edu, o.ransome-kuti.6269@westcliff.edu, otawodi@myharrisburgu.edu, omolayooa15@outlook.com, n.Lesinwa.122@westcliff.edu, toluawesome@gmail.com

## Abstract

In the contemporary era dominated by digital connectivity, the convergence of technology and talent acquisition thrust nursing staffing agencies into the focal point of an escalating threat landscape posed by cyber adversaries. This study explores cybersecurity challenges confronting nursing staffing agencies, examining vulnerabilities, repercussions, and indispensable proactive measures aimed at safeguarding sensitive data. Providing a comprehensive overview, the study sheds light on the increasing frequency and sophistication of cyber threats, underscoring the distinct susceptibility of nursing staffing agencies due to their heavy reliance on online systems. A notable concern within this context is the emergence of insider threats, originating from within the organizational ranks and driven by motivations ranging from negligence to malicious intent. The study places a critical focus on advocating the zero-trust paradigm as a potent cybersecurity strategy, advocating for a steadfast "never trust, always verify" approach. This strategy is deemed paramount for neutralizing insider threats, particularly relevant in an era characterized by the prevalence of remote work and the widespread adoption of cloud migration. Furthermore, the role of technology takes center stage, with a specific emphasis on Human Layer Security (HLS) and machine learning-based analytics, which play pivotal roles in identifying and mitigating insider threats. The study advocates a dynamic organizational methodology that perceives cybersecurity as an evolving process. It urges nursing staffing agencies to fortify their defenses through the implementation of a unified and integrated security program. Additionally, the study proposes advanced cybersecurity measures tailored specifically for nursing staffing agencies. These encompass crucial aspects such as data classification, access control, identity and access management, user activity monitoring, and comprehensive security awareness training. By implementing these recommendations, nursing staffing agencies can confidently navigate the digital landscape, ensuring the protection of sensitive data, maintaining client trust, and cultivating a resilient defense against the ever-evolving spectrum of cyber threats.

**Keywords:** Nursing Staffing Agencies, Insider Threats, Cybersecurity Measures, Zero-Trust Paradigm and Advanced Technologies

**DOI:** 10.7176/JIEA/15-2-03
**Publication date:** May 28th 2025

## 1. Introduction

In an era dominated by digital connectivity, the escalating frequency and sophistication of cyber threats have catapulted cybersecurity to the forefront of concerns for businesses across diverse sectors. The nursing staffing agencies, heavily reliant on online systems, become an immediate target for cybercriminals due to the exposure of sensitive employment documents during a breach (Nasstar, 2020). Recent years have witnessed an increase in cyber-attacks within the health sector in general and nursing staffing agencies in particular, impacting companies globally (Ross et al., 2020). Candidate data is identified as the most crucial intellectual property, and any compromise could cripple the entire operation, leading to long-lasting reputational damage and risks associated with breaching confidential data (Uchendu et al, 2021). Nursing Staffing agencies handle extensive confidential data, including non-public client business details, making them potential targets for cybercriminals seeking competitive advantages or jeopardizing long-term contracts. The exposure of candidate information, including income, contact details, personal history, passport, visa, and financial details, poses significant risks, including ransomware attacks (Morgan, 2017; Markos et al., 2023). The interconnected nature of online business operations and reliance on outsourced IT management further increase the attack surface.

An insider threat, defined as a security threat originating from within an organization, is a growing concern for enterprises, with costs rising by 31% from 2018 to 2020 (Bore, 2020). These threats can be categorized as either malicious or negligent, presenting risks such as sabotage, fraud, intellectual property theft, and espionage (Costa et al., 2016; Pfleeger et al, 2009). The motivations behind insider threats vary, leading to potential harm through actions like neglecting data security or engaging in destructive behaviors such as sabotage or fraud (Elifoglu et al., 2018; Fenstermacher et al., 2022). Insiders, including employees (nurses in context), contractors, and service providers, pose diverse risks based on their roles and access levels. Current employees, exiting employees, and former employees represent different levels of risk, and their motivations may range from revenge to market information to competitors (Bosworth et al., 2014; Pfleeger et al., 2009).

Cybersecurity is critical in protecting against various threats (Borky et al., 2019). As shown in Fig. 1, malicious software, like malware, poses a risk to computer systems and requires defenses such as anti-malware tools and firewalls. Distributed denial of service (DDoS) attacks can disrupt operations, especially impactful for recruitment agencies heavily reliant on online services. Phishing scams, targeting agencies with regular email communication, aiming to deceive and gain sensitive information (Nasstar, 2020). Ransomware adds another layer of risk, with cybercriminals aware of the valuable data held by recruitment agencies. Human error, often the root of cyber-attacks, includes actions like clicking on phishing email links. Restricting access to sensitive data is crucial, considering the risk of data theft by departing employees (Haney & Lutters, 2019). Cybersecurity training for all staff is vital to prevent errors, covering aspects like recognizing phishing threats (Haney & Lutters, 2019). Outdated software, a vulnerability exploited by hackers, necessitates regular updates and transitioning to secure systems. Establishing comprehensive cybersecurity policies, encompassing areas like Bring Your Own Device (BYOD), remote work, and password control, is essential for overall protection (Nasstar, 2020).

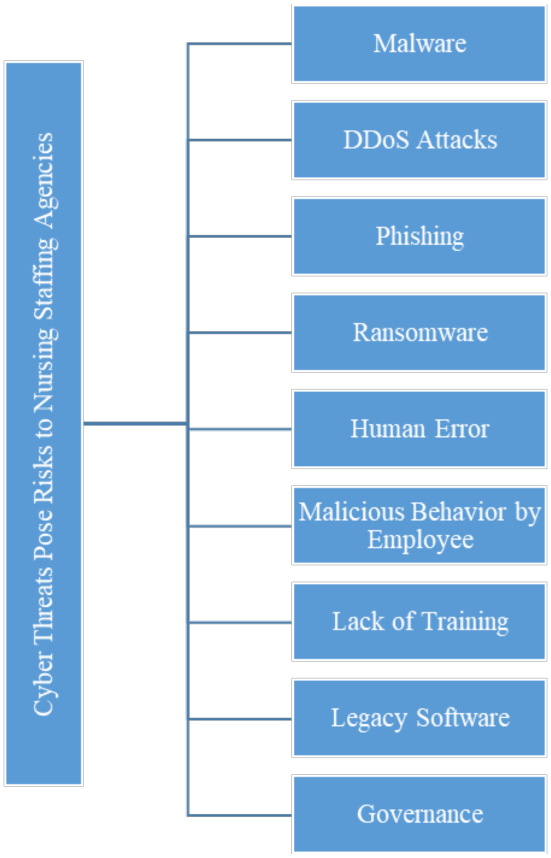

**Fig. 1: Various Cyber Threats Pose Risks to Nursing Staffing Agencies**

In addressing the ongoing labor shortage in the labor force, nursing staffing agencies offer a strategic solution (Dawson & Thomson, 2018). These agencies provide flexibility, cost savings, and expedited hiring processes, allowing organizations to navigate the digital landscape securely and efficiently (Cobb, 2016). This discourse examines the landscape of cybersecurity challenges faced by the staffing industries, exploring the vulnerabilities, repercussions, and proactive measures essential for safeguarding sensitive data.

### *1.1 Understanding Insider Threats in Nursing Staffing Agencies*

In the era of the internet, life has undeniably become more convenient, offering real-time access to news, 24/7 financial connectivity, and the luxury of doorstep grocery deliveries (Reed, 2018). However, this digital ease is accompanied by increased complexities, particularly when cybercriminals gain access to sensitive information, making life difficult swiftly. Even the largest staffing organizations are not exempt from the looming threat of cyber-attacks. The reality is that a robust defense minimizing risks is crucial for most companies. Human Resources (HR) departments and staffing agencies, in particular, find themselves highly vulnerable to cyber-attacks due to the nature of their operations (Fisher et al., 2021).

For instance, nursing staffing agencies, pivotal in connecting employers with qualified candidates, face a growing threat from insider threats (ITs) due to their unique operational model. The intentional or unintentional misuse of privileged access poses risks such as data exfiltration, identity theft, sabotage, and financial fraud, leading to severe reputational and financial damage (Markos et al., 2023). Nicolaou et al. (2020) highlight a rising trend in insider involvement in data breaches, reaching 28% according to the latest Data Breach Investigations Report (DBIR) by Verizon. Internal actors, including employees, contribute significantly to security incidents, emphasizing the need for robust detection methods (Baker et al., 2011). Insider threats incur substantial costs, with a 31% increase in the global average cost over the last two years, reaching $11.45 million (Saxena et al., 2020). The European Union Agency for Cybersecurity identifies key incidents, including privilege abuse and data mishandling. Insider attacks extend beyond the private sector, affecting government institutions and critical infrastructures (Saxena et al., 2020). The threat is categorized as malicious, compromised, and careless insiders, each requiring distinct defense strategies (Saxena et al., 2020). Abnormal activities serve as potential indicators, and detection involves understanding motivations and characteristics unique to each type (Marinos & Government Accountability Office Washington DC., 2020). In their study, Greitzer et al. (2019) stress the financial consequences, averaging $8.76 million per organization. Insider threat programs (ITPs) aim to detect and mitigate risks, often incorporating technical solutions and behavioral analysis. However, behavioral analysis integration remains limited, highlighting the need for a comprehensive approach. The maturity of ITPs varies, with optimized programs featuring multidisciplinary teams and stakeholder collaboration. To enhance threat assessment, organizations should standardize terms, emphasize comprehensive assessment programs, and integrate knowledge bases like SOFIT (Homoliak et al., 2019). Continuous improvement is crucial for addressing evolving threats and maintaining ITP effectiveness.

#### 1.1.1 Extant Literature on Insider Threats

Nursing staffing agencies, handling sensitive data like credit card information and personal nurse details, are common targets for cybercriminals (Dimuna, 2020). Vulnerabilities arise from accidental incidents and employee misconduct, emphasizing the critical need for robust cybersecurity measures (Lahcen et al, 2020). Implementing effective safeguards and exploring insurance policies are essential for minimizing the risks and potential fallout of a cyber-attack (Falco & Rosenbach, 2022). Nursing staffing agencies, dealing with extensive sensitive information, are vulnerable to cyber threats, especially due to the rise of remote work models (Haney & Lutters, 2019). They receive a massive influx of emails and file attachments, making them attractive targets for cybercriminals seeking unauthorized access (Haney & Lutters, 2019). The evolving landscape of the internet and the prevalence of various cyber-attack tactics further accentuate the need for heightened cybersecurity measures (Fisher et al., 2021). Surprisingly, the majority of the nursing staffing industry lacks comprehensive standards and guidelines from professional bodies regarding cybersecurity and information security (Uchendu et al, 2021). While GDPR compliance is supported, there is a noticeable gap in establishing industry-wide security standards. A proactive approach, including awareness campaigns, ongoing governance, insider threat awareness, and robust Incident Response Plans, is essential to enhance security controls. Businesses often hire temporary workers to manage increased workloads, particularly during peak periods like December. However, a study by Avecto reveals a cybersecurity risk, as 72 percent of temporary hires receive admin privileges on the company network (Elifoglu et al., 2018). This poses a potential "keys to the kingdom" scenario, emphasizing the need for a granular approach to admin rights, granting access to applications rather than users (Argaw et al., 2020).

Restricting temporary workers' network access to the minimum necessary and promptly revoking it upon the end of their employment term is crucial to mitigate insider threat risks.

## 2. Advanced Cybersecurity Measures

Cybersecurity has always been crucial, but in today's advanced technological landscape, where cyber threats have evolved in tandem with technological progress, its significance has escalated. With a substantial amount of data being stored online and processes transitioning from manual to digital, the need for robust cybersecurity measures has never been more vital (Haney & Lutters, 2019). This holds particularly true for companies involved in hiring and recruiting, where vast amounts of sensitive data are exchanged. Even after an employee is hired, the digital exchange of information during onboarding, including company details, passwords, security protocols, and financial data, creates vulnerabilities that cybercriminals seek to exploit. While recruitment agencies are currently prime targets due to the digital nature of hiring processes, adherence to cybersecurity best practices can effectively thwart threats (Sykes Jr, 2014). Vigilance in scrutinizing emails, verifying applicants, encrypting data, and employing dedicated cybersecurity teams are crucial steps in safeguarding sensitive data and ensuring the integrity of recruitment operations (Haney & Lutters, 2019). Setting tolerable levels of risk requires a well-executed business impact analysis to quantify impacts and define loss thresholds. The lack of such analyses can lead to the transfer of risks to consumers through price increases (Sarkar et al., 2010). To manage the threat posed by contingent staff, human resource security management and control activities are recommended. This includes pre-hire background checks, proper allocation of security access rights, regular reviews, and immediate revocation of access rights upon termination (Sarkar, 2010).

### 2.1 *Advanced Cyber-security Measures for Mitigation:*

Insider threats, emanating from employees, temporary workers, and contractors, have become a significant concern for businesses, necessitating robust risk-management strategies. A multifaceted approach is crucial to address the diverse manifestations of insider threats, ranging from unintentional errors to deliberate acts of theft or sabotage. To address these challenges, nursing staffing agencies need to implement a comprehensive cyber-security program that incorporates advanced measures specifically tailored to IT mitigation. Here are the proactive measures to fortify nursing staffing agencies against cyber threats and ensure data safety for clients and candidates (Fisher et al., 2021; Buffington, 2023):

- **Data Classification and Access Control:** Implement robust data classification procedures to identify and protect sensitive information. Enforce the principle of least privilege, granting access only to the data employees need to perform their jobs (Ross et al., 2020).
- **Identity and Access Management (IAM):** Utilize multi-factor authentication and strong password policies to prevent unauthorized access. Implement an IAM system to manage user accounts and privileges effectively, including temporary worker accounts (Falco & Rosenbach, 2022).
- **User Activity Monitoring (UAM):** Continuously monitor user activity for anomalous behavior, flagging suspicious actions like unauthorized data downloads or attempts to access restricted files. This can help detect potential ITs before they cause considerable damage (Sykes Jr, 2014).
- **Security Awareness Training:** Regularly train all employees, including temporary workers, in cyber-security best practices and the importance of reporting suspicious activity. This fosters a culture of security awareness and encourages employees to become active participants in IT mitigation (Bore, 2020).
- **Deeper Background Checks:** Consider conducting more thorough background checks, particularly for high-risk roles or individuals with access to sensitive data. This can help identify potential red flags that may indicate an increased risk of IT (Buffington, 2023).

Employee theft, contributing to annual losses of $50 billion, is a significant concern for businesses (Farahbod, 2020; Hunker & Probst, 2011). Nursing staffing agencies, facing unique challenges due to high turnover rates, need effective strategies to protect assets, as their clients' property is also at risk (Hunker & Probst, 2011). Mitigating these risks requires due diligence in cybersecurity practices, certifications, and audits, incorporated into contracts with nursing staffing agencies (Argaw et al., 2020).

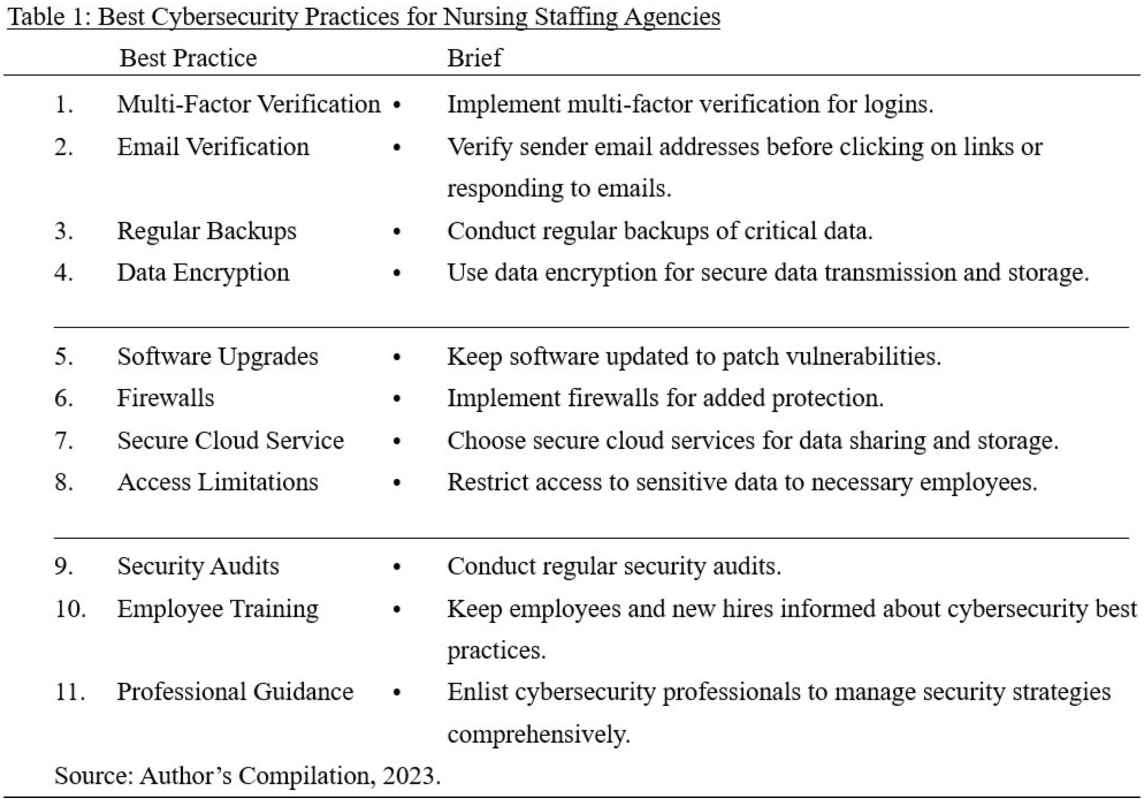

Table 1: Best Cybersecurity Practices for Nursing Staffing Agencies

| | Best Practice | Brief |
|---|---|---|
| 1. | Multi-Factor Verification | • Implement multi-factor verification for logins. |
| 2. | Email Verification | • Verify sender email addresses before clicking on links or responding to emails. |
| 3. | Regular Backups | • Conduct regular backups of critical data. |
| 4. | Data Encryption | • Use data encryption for secure data transmission and storage. |
| 5. | Software Upgrades | • Keep software updated to patch vulnerabilities. |
| 6. | Firewalls | • Implement firewalls for added protection. |
| 7. | Secure Cloud Service | • Choose secure cloud services for data sharing and storage. |
| 8. | Access Limitations | • Restrict access to sensitive data to necessary employees. |
| 9. | Security Audits | • Conduct regular security audits. |
| 10. | Employee Training | • Keep employees and new hires informed about cybersecurity best practices. |
| 11. | Professional Guidance | • Enlist cybersecurity professionals to manage security strategies comprehensively. |

Source: Author's Compilation, 2023.

Therefore, cybersecurity should be viewed as a dynamic organizational methodology. As technology progresses, so do cyber threats (Fisher et al., 2021). Regular reassessment and redirection of security policies are essential to keep pace with evolving risks, preventing cyberattacks from becoming one attack too many.

### 2.2. Fortifying Security Resilience: The Zero-Trust Paradigm and Comprehensive Insider Threat Strategies

This section investigates the proactive approach of the zero-trust model in cybersecurity, examining its significance in neutralizing insider threats. From understanding various manifestations of insider risks to deploying innovative solutions like Human Layer Security (HLS) and conducting thorough background checks, this section explores a comprehensive personnel security strategy. It emphasizes the need for ongoing screening, legal compliance, and the integration of modern technology, such as machine learning-based user behavior analytics, to create a unified and robust defense against insider threats.

The zero-trust approach is effective in cybersecurity by adopting a "never trust, always verify" stance, subjecting users, applications, devices, networks, and processes to rigorous screening and continuous verification (Stern et al., 2021). This strategy is crucial in neutralizing insider threats, where individuals within an organization pose potential security risks due to their access to sensitive data. Insider threats can include current or former employees, partners, contractors, or temporary staff who may be malicious or inadvertently risky. The zero-trust model becomes especially vital with the increasing prevalence of remote work and the migration of workloads to the cloud. By deploying this architecture, organizations can detect exploits, limit disruptions related to data breaches, enhance cyber resiliency, and provide sophisticated protection to resources and users.

Insider threats encompass a range of risks, from unintentional errors to intentional malicious actions. Homoliak et al. (2019) suggests understanding various manifestations and tailoring responses accordingly, this involves demystifying preconceived fears related to employee trust and fostering sustained behavioral and cultural changes. Clear and transparent communication about program intentions, objectives, and employee requirements is crucial for success, reducing insider risk and enhancing overall organizational safety (Homoliak et al., 2019). To address these challenges, a comprehensive personnel security strategy is essential, encompassing awareness training and machine learning-based solutions (Zimmermann & Renaud, 2019). Human Layer Security (HLS) is an innovative approach that studies human behavior patterns, creating unique security identities and automatically detecting and preventing attacks.

Background checks, conducted under the Fair Credit Reporting Act (FCRA), involve verifying applicant-provided information and searching public or private records. Criminal record checks are particularly important, but employers must comply with Equal Employment Opportunity (EEO) laws and Ban the Box rules when considering criminal records (Jeong & Zo, 2021). Litigation, regulation, and legislation related to background checks have increased, necessitating legal compliance expertise and stringent data security measures. Even with background checks, predicting future employee behavior remains challenging. Employers are encouraged to supplement pre-employment background checks with ongoing or continuous screening, fostering an environment of control and physical safety (Jeong & Zo, 2021). Insider threats can emerge even with "good hires," especially among employees with substantial authority or access to sensitive information. Unpredictable and secret risks, such as financial issues or political agendas, may also pose threats. Employers can face post-hire surprises, such as discovering new information about an employee's background. A well-thought-out pre-employment screening program, including policies, practices, and procedures, can help minimize surprises (Jeong & Zo, 2021). Screening tools for detecting insider threats include ongoing evaluation, re-enactment screenings, credit reports, social media background checks, and screening current workers or newly acquired workforce. Continuous evaluation after hiring raises legal implications, requiring careful consideration and documentation.

Security awareness training plays a crucial role in minimizing human errors, responsible for 85% of breaches (Ayereby, 2018; Meehan et al., 2021). Compensating controls, such as Acceptable Use Policies and job rotation, contribute to overall security. However, addressing insider threats requires a unified and integrated security program that considers people, processes, and tools (Bore, 2020). Modern technology and analytics, particularly machine learning-based user behavior analytics, are proving effective in identifying and mitigating insider threats, emphasizing the importance of user-friendly environments to encourage adherence to security protocols (Pfleeger et al., 2009).

## 3.0 Conclusion

Combating insider threats requires a comprehensive and adaptive approach, encompassing technical solutions, human factors, and organizational policies. Understanding the evolving nature of these threats and implementing proactive measures are pivotal for organizations to safeguard their assets and maintain the trust of clients and consumers. Therefore, the recruitment sector faces formidable challenges in safeguarding sensitive data from cyber threats. A proactive and comprehensive approach, encompassing employee training, governance policies, and collaboration with cybersecurity experts, is imperative. Embracing cybersecurity as a collective responsibility is not only a necessity but also a strategic move to fortify relationships with clients and candidates in the face of evolving cyber threats.

Based on the findings of the study, the following recommendations are made to fortify the defenses:

1. Implement Comprehensive Cybersecurity Policies: Develop and enforce robust cybersecurity policies covering data classification, access control, and secure cloud services. Regularly update these policies to address emerging threats and technological advancements.

2. Adopt the Zero-Trust Paradigm: Embrace the zero-trust approach as a foundational principle, incorporating continuous verification and strict access controls. This is particularly crucial in the context of remote work and cloud-based operations.

3. Enhance User Awareness and Training: Prioritize ongoing cybersecurity training for all employees, including temporary staff. Foster a culture of security awareness to empower individuals to recognize and report potential threats.

4. Invest in Advanced Technologies: Leverage innovative solutions such as Human Layer Security (HLS) and machine learning-based analytics to detect and prevent insider threats. Stay abreast of technological advancements to adapt defenses to evolving risks.

5. Conduct Thorough Background Checks: Strengthen pre-employment screening programs, supplementing traditional background checks with ongoing evaluations. Consider the legal implications of continuous evaluation and ensure careful documentation.

6. Collaborate with Cybersecurity Professionals: Enlist the expertise of cybersecurity professionals to guide the development and implementation of security strategies. Regular security audits can provide valuable insights into the effectiveness of existing measures.

Therefore, by implementing these recommendations and fortifying security resilience, nursing staffing agencies can navigate the digital landscape securely, ensuring the protection of sensitive data, maintaining client trust, and fostering a resilient defense against the ever-evolving spectrum of cyber threats.

## References

Argaw, S.T., Troncoso-Pastoriza, J.R., Lacey, D., Florin, M.V., Calcavecchia, F., Anderson, D. & Flahault, A., 2020. Cybersecurity of hospitals: discussing the challenges and working towards mitigating the risks. *BMC Medical Informatics and Decision Making*, 20, pp.1-10. https://doi.org/10.1186/s12911-020-01161-7

Ayereby, M.P.M., 2018. Overcoming data breaches and human factors in minimizing threats to cyber-security ecosystems. *Doctoral dissertation*, Walden University.

Baker, W., Goudie, M., Hutton, A., Hylender, C.D., Niemantsverdriet, J., Novak, C. & Neal, C., 2011. 2011 data breach investigations report. Verizon RISK Team. Available at: www.verizonbusiness.com/resources/reports/rp_databreach-investigationsreport-2011_en_xg.pdf [Accessed 13 May 2025].

Bore, J., 2020. Insider threat. In: *Cyber Defense in the Age of AI, Smart Societies and Augmented Humanity*, pp.431-450. https://doi.org/10.1007/978-3-030-35746-7_19

Borky, J.M., Bradley, T.H., Borky, J.M. & Bradley, T.H., 2019. Protecting information with cybersecurity. In: *Effective Model-Based Systems Engineering*, pp.345-404. https://doi.org/10.1007/978-3-319-95669-5_10

Bosworth, S., Kabay, M.E., Whyne, E. & Tagg, G., 2014. The insider threat. In: *Computer Security Handbook*, pp.421-432. John Wiley & Sons, Inc.

Cobb, S., 2016. Mind this gap: Criminal hacking and the global cybersecurity skills shortage, a critical analysis. In: *Virus Bulletin Conference*, pp.1-8.

Costa, D.L., Albrethsen, M.J., Collins, M.L., Perl, S.J., Silowash, G.J. & Spooner, D.L., 2016. An insider threat indicator ontology. SEI, Pittsburgh, PA, USA, Rep. CMU/SEI-007.

Dawson, J. & Thomson, R., 2018. The future cybersecurity workforce: Going beyond technical skills for successful cyber performance. *Frontiers in Psychology*, 9, p.744. https://doi.org/10.3389/fpsyg.2018.00744

Dimuna, L.U., 2020. A qualitative study of cybersecurity strategies to reduce medical identity theft focusing on the managers' lived experiences. *Doctoral dissertation*, Colorado Technical University.

Elifoglu, I.H., Abel, I. & Taşseven, Ö., 2018. Minimizing insider threat risk with behavioral monitoring. *Review of Business*, 38(2), pp.61-73. ISSN: 0034-6454.

Falco, G.J. & Rosenbach, E., 2022. *Confronting cyber risk: An embedded endurance strategy for cybersecurity*. Oxford University Press.

Farahbod, K., Shayo, C. & Varzandeh, J., 2020. Cybersecurity indices and cybercrime annual loss and economic impacts. *Journal of Business and Behavioral Sciences*, 32(1), pp.63-71.

Fenstermacher, L., Larson, K., Vitiello, C., Shellman, S. & Levey, B., 2022. Analytics for early detection of insider threat. In: *Signal Processing, Sensor/Information Fusion, and Target Recognition XXXI*, Vol. 12122, pp.172-187. SPIE. https://doi.org/10.1117/12.2624111

Fisher, R., Porod, C. & Peterson, S., 2021. Motivating employees and organizations to adopt a cybersecurity-focused culture. *Journal of Organizational Psychology*, 21(1), pp.114-131.

Greitzer, F.L., Purl, J., Leong, Y.M. & Sticha, P.J., 2019. Positioning your organization to respond to insider threats. *IEEE Engineering Management Review*, 47(2), pp.75-83. https://doi:10.1109/EMR.2019.2914612

Haney, J.M. & Lutters, W.G., 2019. Motivating cybersecurity advocates: Implications for recruitment and retention. In: *Proceedings of the 2019 on Computers and People Research Conference*, pp.109-117. https://doi.org/10.1145/3322385.3322388

Homoliak, I., Toffalini, F., Guarnizo, J., Elovici, Y. & Ochoa, M., 2019. Insight into insiders and IT: A survey of insider threat taxonomies, analysis, modeling, and countermeasures. *ACM Computing Surveys (CSUR)*, 52(2), pp.1-40. https://doi.org/10.1145/3303771

Hunker, J. & Probst, C.W., 2011. Insiders and insider threats – an overview of definitions and mitigation techniques. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, 2(1), pp.4-27. Available at: https://isyou.info/jowua/papers/jowua-v2n1-1.pdf [Accessed 13 May 2025].

Jeong, M. & Zo, H., 2021. Preventing insider threats to enhance organizational security: The role of opportunity-reducing techniques. *Telematics and Informatics*, 63, p.101670.

https://doi.org/10.1016/j.tele.2021.101670

Maalem Lahcen, R.A., Caulkins, B., Mohapatra, R. & Kumar, M., 2020. Review and insight on the behavioral aspects of cybersecurity. *Cybersecurity*, 3(1), pp.1-18. https://doi.org/10.1186/s42400-020-00050-w

Marinos, N. & Government Accountability Office Washington DC., 2020. Cybersecurity: Clarity of leadership urgently needed to fully implement the national strategy.

Markos, E., Peña, P., Labrecque, L.I. & Swani, K., 2023. Are data breaches the new norm? Exploring data breach trends, consumer sentiment, and responses to security invasions. *Journal of Consumer Affairs*, 57(3), pp.1089-1119. https://doi.org/10.1111/joca.12554

Matt Buffington, 2023. Cybersecurity and your staffing agency. Available at: https://www.linkedin.com/pulse/importance-cybersecurity-your-staffing-agency-matt-buffington/ [Accessed 13 May 2025].

Meehan, J., Wilson, B. & Pinto, A., 2021. DBIR - 2021 data breach investigations report – Verizon. Available at: https://enterprise.verizon.com/content/verizonenterprise/us/en/index/resources/reports/2021-data-breachinvestigations-report.pdf [Accessed 13 May 2025].

Morgan, S., 2017. Global Ransomware damage costs predicted to exceed $8 Billion in 2018. California: Cyber Security Ventures.

Nasstar, 2020. Biggest cyber security threats to the recruitment sector. APSCo Global. Available at: https://www.apsco.org/resource/biggest-cyber-security-threats-to-the-recruitment-sector.html [Accessed 13 May 2025].

Nicolaou, A., Shiaeles, S. & Savage, N., 2020. Mitigating insider threats using bio-inspired models. *Applied Sciences*, 10(15), p.5046. https://doi.org/10.3390/app10155046

Pfleeger, S.L., Predd, J.B., Hunker, J. & Bulford, C., 2009. Insiders behaving badly: Addressing bad actors and their actions. *IEEE Transactions on Information Forensics and Security*, 5(1), pp.169-179. https://doi.org/10.1109/TIFS.2009.2039591

Reed, T.V., 2018. *Digitized lives: Culture, power and social change in the internet era*. Routledge.

Ross, R., Pillitteri, V., Guissanie, G., Wagner, R., Graubart, R. & Bodeau, D., 2020. Enhanced security requirements for protecting controlled unclassified information: A supplement to NIST Special Publication 800-171 (Final Public Draft) (No. NIST Special Publication (SP) 800-172 (Draft)). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-172-draft

Sarkar, K.R., 2010. Assessing insider threats to information security using technical, behavioral, and organizational measures. *Information Security Technical Report*, 15(3), pp.112-133. https://doi.org/10.1016/j.istr.2010.11.002

Saxena, N., Hayes, E., Bertino, E., Ojo, P., Choo, K.K.R. & Burnap, P., 2020. Impact and key challenges of insider threats on organizations and critical businesses. *Electronics*, 9(9), p.1460. https://doi:10.3390/electronics9091460

Stern, A., Wang, H., Rahman, F., Farahmandi, F. & Tehranipoor, M., 2021. ACED-IT: Assuring confidential electronic design against insider threats in a zero-trust environment. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 41(10), pp.3202-3215. https://doi.org/10.1109/TCAD.2021.3127864

Sykes Jr, D.N., 2014. Prevention of internal cyber-security threats. *Doctoral dissertation*, Walden University.

Uchendu, B., Nurse, J.R., Bada, M. & Furnell, S., 2021. Developing a cyber security culture: Current practices and future needs. *Computers & Security*, 109, p.102387. https://doi.org/10.1016/j.cose.2021.102387

Zimmermann, V. & Renaud, K., 2019. Moving from a ‘human-as-problem’ to a ‘human-as-solution’ cybersecurity mindset. *International Journal of Human-Computer Studies*, 131, pp.169-187. https://doi.org/10.1016/j.ijhcs.2019.05.005