# Risk Assessment of the 2024 NHS Cyber Attack Using NIST

SENZOSENKOSI SIPHIWO SHONGWE 201603562

# Executive summary

This report presents a comprehensive risk analysis of the 2024 cyber attack on the United Kingdom's National Health Service (NHS), focusing specifically on the incident at Wirral University Teaching Hospital in Merseyside. On 26 November 2024, the hospital experienced a significant ransomware attack that disrupted critical IT systems, delayed diagnostics, and compromised patient safety (Tharun et al., 2025). This event was part of a broader pattern of cyber threats targeting healthcare infrastructure globally, underscoring the urgent need for structured, proactive risk management in the sector (Periculo, 2024).

The primary objective of this report is to identify, evaluate, and mitigate cybersecurity risks exposed during the NHS incident using the National Institute of Standards and Technology (NIST). NIST was selected for its incident-driven, repeatable framework that aligns with healthcare-specific regulatory requirements such as the General Data Protection Regulation and NHS Cyber Resilience standards (Srivastava et al., 2024). The methodology supports both qualitative and semi-quantitative risk assessments, making it ideal for evaluating threats to confidentiality, integrity, and availability in critical environments.

The report begins by defining the scope of the assessment, which includes hospital IT systems, third-party vendor platforms, and patient data repositories. Key stakeholders such as NHS cybersecurity teams, hospital administrators, clinical staff, and regulatory bodies are identified to ensure a holistic understanding of the risk landscape. Critical assets are categorized based on their operational importance and exposure to cyber threats.

A risk matrix is developed to prioritize threats based on their likelihood and impact. For example, patient data repositories exposed to ransomware are classified as "Critical" risk due to their high likelihood and severe impact. Clinical systems vulnerable to insider threats and vendor platforms susceptible to phishing are also rated as "High" risk. The matrix provides a clear visual representation of risk levels across different assets and threat vectors.

To address these risks, the report proposes a set of targeted mitigation strategies. These include implementing multi-factor authentication across all administrative and clinical systems, integrating a Security Operations Centre for real-time monitoring, automating patch management to reduce exposure windows, segmenting networks to isolate critical systems, conducting regular vendor security audits, and maintaining offline, immutable backups of essential data. Incident response drills are also recommended to test organizational readiness and improve recovery protocols (NCSC, 2024).

The report critically evaluates the effectiveness of these controls, acknowledging both their strengths and limitations. While the proposed measures significantly enhance resilience and regulatory compliance, challenges remain in areas such as predictive threat modelling, vendor accountability, and forensic traceability. Recommendations for improvement include integrating machine learning-based anomaly detection, simulating ransomware scenarios in containerized environments, and expanding the risk framework to include real-time alerting and forensic logging.

In conclusion, the application of the NIST methodology to the 2024 NHS cyber attack provides a structured and actionable approach to risk management in healthcare. The proposed controls, if properly implemented, will strengthen the NHS's ability to prevent, detect, and respond to future cyber incidents, thereby safeguarding patient data, maintaining operational continuity, and restoring public trust in the system's cyber resilience.

# Introduction

Cybersecurity has become a critical concern in healthcare as hospitals increasingly depend on interconnected digital systems for diagnostics, patient records, and administrative operations. The 2024 ransomware attack on Wirral University Teaching Hospital in Merseyside, UK, exemplifies the vulnerabilities inherent in healthcare infrastructure and the potentially devastating consequences of cyber threats on patient safety and service continuity (Meshkat and Miller, 2022).

This report aims to conduct a structured risk analysis of the NHS cyber attack using the National Institute of Standards and Technology methodology. The objective is to systematically identify threat sources, assess vulnerabilities, estimate the likelihood and impact of adverse events, and propose targeted mitigation strategies. The analysis focuses on critical assets such as hospital IT systems, third-party vendor platforms, and patient data repositories.

The chosen approach leverages NIST's seven-step framework, which is well-suited to incident driven assessments in critical infrastructure sectors like healthcare. It supports both qualitative and semi-quantitative risk evaluation and aligns with regulatory standards including the General Data Protection Regulation and NHS Cyber Resilience guidelines (NIST, 2012) By applying this methodology to the Wirral case study, the report seeks to enhance the NHS's ability to prevent, detect, and respond to future cyber incidents.

# Problem statement

The 2024 ransomware attack on Wirral University Teaching Hospital revealed critical weaknesses in the cybersecurity posture of healthcare institutions. The incident disrupted essential services, delayed diagnostics, and exposed sensitive patient data, demonstrating the sector's vulnerability to targeted cyber threats (Getronics, 2024).

The specific risk analysis problem addressed in this report is the NHS's limited ability to proactively identify and mitigate cybersecurity risks across its digital infrastructure. This includes inadequate network segmentation, delayed patch management, and insufficient oversight of third-party vendors factors that collectively increased the likelihood and impact of the attack (NCSC, 2024).

Healthcare environments face unique challenges due to their reliance on legacy systems, continuous service delivery, and complex data flows. These conditions amplify the consequences of cyber incidents, making structured risk assessment essential. Therefore, this report applies the NIST framework to systematically evaluate threats, vulnerabilities, and impacts, and to develop targeted mitigation strategies that enhance resilience, regulatory compliance, and patient safety (NIST, 2012).

# Overview of the Developed Risk Analysis Tool

The NHS Risk Analysis and Scoring Tool  will be developed in alignment with the National Institute of Standards and Technology, providing a structured and repeatable approach to identifying, analysing, and prioritising cybersecurity risks within healthcare environments. The tool is designed to assist security analysts and IT managers in systematically assessing risks across various NHS departments and information systems, particularly in settings where patient data confidentiality, system integrity, and service availability are critical.

NHS Risk Analysis and Scoring Tool (NRAST), combines quantitative scoring methods, such as numerical weightings for likelihood and impact, with qualitative expert judgment, enabling a

comprehensive evaluation of potential threats. This dual approach ensures that both measurable technical vulnerabilities and contextual operational risks are adequately represented in the assessment process. The tool is also modular and adaptable, allowing it to be customised according to the operational requirements, infrastructure complexity, and digital maturity of different NHS trusts or healthcare facilities (NCSC, 2024).

The tool will operate through a three-phase process designed to reflect the NIST risk assessment lifecycle. In Phase 1- Risk Identification, the tool gathers information on critical assets, associated threats, vulnerabilities, and affected systems to produce an initial risk register. Phase 2- Risk Evaluation involves assigning weighted scores to parameters such as likelihood, impact, and control effectiveness, generating a quantified risk rating for each identified threat. Phase 3- Risk Response focuses on developing mitigation, transfer, or acceptance strategies, culminating in a prioritised risk treatment plan (NIST, 2012).

By following these structured phases, the NRAST tool aligns with NIST's core principles of risk framing, assessment, and communication, supporting consistent documentation, prioritisation, and reporting of cybersecurity risks. This structured approach enhances the NHS's capacity to make informed, data-driven decisions to safeguard its critical information infrastructure and maintain public trust in healthcare service delivery (Mohamed Mohideen et al., 2024).

# Methodology Used

The NIST methodology was adopted as the foundational framework for this risk analysis because it offers a comprehensive, systematic, and adaptable approach to identifying, assessing, and managing cybersecurity risks across critical infrastructure sectors, including healthcare. This methodology is widely recognised as an international benchmark for risk management due to its ability to integrate both technical and organisational factors into the assessment process (Mohamed Mohideen et al., 2024).

### *Sector Suitability*

The NIST framework is particularly suitable for the healthcare sector, as it was designed to support risk assessment in environments where safety, confidentiality, and availability are paramount. The NHS, as part of the United Kingdom's critical healthcare infrastructure, depends on uninterrupted access to digital systems for patient care, diagnostics, and administrative operations. Disruptions to these systems, such as those experienced during the 2024 ransomware attack at Wirral University Teaching Hospital, can have life-threatening consequences (Tharun et al., 2025). The NIST methodology directly supports the evaluation of such high-stakes risks by providing structured guidance for analysing system vulnerabilities, threat likelihood, and impact severity. Furthermore, it aligns closely with NHS Digital and National Cyber Security Centre standards for cyber resilience, which emphasise proactive threat identification and mitigation (National Cyber Security Centre, 2024).

### *Comprehensiveness*

A key justification for using NIST lies in its comprehensive coverage of the risk management lifecycle. Unlike narrower frameworks that focus solely on technical vulnerabilities, NIST incorporates an end-to-end perspective encompassing threat identification, likelihood estimation, impact analysis, and continuous monitoring. This holistic approach ensures that both technical and human elements of risk, such as insider threats, vendor weaknesses, and operational dependencies, are adequately considered (NIST, 2012). The framework also supports integration with automated risk scoring

mechanisms, as implemented within the NHS Risk Analysis and Scoring Tool (NRAST), allowing for consistent documentation and comparison of risk exposure across departments.

### *Compatibility and Interoperability*

Another strength of the NIST methodology is its interoperability with other internationally recognised standards. It aligns with ISO/IEC 27005, which focuses on information security risk management, and complements legal and regulatory requirements such as the General Data Protection Regulation. This compatibility ensures that risk assessments conducted under NIST can be integrated into broader governance and compliance initiatives without redundancy. Additionally, NIST's alignment with the NHS Cyber Assessment Framework enables healthcare organisations to map assessment outcomes directly to NHS cyber maturity indicators, simplifying compliance reporting and facilitating policy harmonisation (Calvo et al., 2025).

### *Evidence-Based and Data-Driven*

NIST promotes an evidence-based, data-driven approach to risk assessment, making it ideal for environments that generate large volumes of operational and security data. By allowing both quantitative and qualitative inputs, the framework supports a nuanced understanding of risk exposure. In this study, quantitative data, such as ransomware frequency, system vulnerability counts, and downtime metrics were combined with qualitative insights from incident response personnel and IT managers to generate balanced, accurate risk profiles (Tharun et al., 2025).

### *The Five Stages of the NIST Risk Assessment Process*

Each stage of the NIST methodology contributes directly to the operational design of the NRAST tool (Abdi, Bennouri and Keane, 2024):

1. **Prepare for Assessment** – Define scope, boundaries, and objectives. For the NHS case study, this included hospital networks, clinical systems, and third-party services. Stakeholders such as IT administrators, cybersecurity officers, and external vendors were identified to ensure accountability and data accuracy.

2. **Conduct Assessment** – Identify threats, vulnerabilities, and potential impact scenarios. NRAST uses predefined questions and weighted scoring to calculate Total Risk (TR) and Residual Risk (RR), forming the basis of the risk register.

3. **Communicate Results** – Document and present findings in actionable formats. Within the NHS context, results are visualised through heat maps and dashboards, enabling rapid identification of high-risk areas.

4. **Maintain Assessment** – Emphasise ongoing monitoring and periodic reviews. NRAST supports dynamic updates to risk data and tracks how residual risks evolve post-mitigation.

5. **Implement Risk Response** – Develop and execute treatment plans. NRAST suggests control strategies mitigation, transfer, or acceptance based on residual risk severity. These are mapped to NIST 5 controls to ensure best practice alignment (NIST, 2020).

By aligning NRAST's workflow with the NIST model, the assessment process becomes repeatable, evidence-based, and measurable ensuring consistency and traceability across multiple NHS assessments.

### *Detailed Description of the Tool*

The NHS Risk Analysis and Scoring Tool (NRAST) evaluates cybersecurity risks using a weighted, semi-quantitative scoring model that is derived from the principles outlined in the NIST risk assessment framework and best practices from current industry methodologies (NIST, 2020). The purpose of this model is to transform complex, multifactorial cybersecurity risks into measurable values that can be systematically compared, prioritised, and managed. By applying numerical weights and mathematical formulas, the tool enables objective risk evaluation and supports evidence-based decision-making across NHS facilities. At its core, the NRAST tool utilises three principal parameters: Likelihood (L), Impact (I), and Control Effectiveness (C). Each of these parameters contributes to the calculation of both the Total Risk (TR) and the Residual Risk (RR).

Likelihood (L) represents the probability that a specific threat will successfully exploit a vulnerability within a given system. It is measured on a five-point scale ranging from 1 (Very Low), indicating minimal probability of occurrence, to 5 (Very High), indicating that the threat is almost certain to occur. This parameter considers factors such as historical incident frequency, system exposure level, and the presence of threat actors targeting the healthcare sector (Getronics, 2024).

Impact (I) quantifies the potential consequences of a successful attack on the three pillars of information security, confidentiality, integrity, and availability. It is also rated on a five-point scale from 1 (Negligible impact) to 5 (Catastrophic impact), where the highest rating denotes severe outcomes such as prolonged service outages, patient data loss, or compromise of life-critical systems (Clark et al., 2025)

Control Effectiveness (C) measures the strength and adequacy of existing security controls implemented to protect systems or data. This value is expressed as a decimal between 0.1 and 1.0, where higher values indicate more effective controls and lower values represent weak or incomplete security measures. This parameter accounts for factors such as the presence of multi-factor authentication, regular patch management, encryption standards, and employee awareness training (NHS Digital, 2023).

The tool employs two key formulas derived from NIST's quantitative risk management approach to calculate the Total Risk (TR) and Residual Risk (RR).

The Total Risk (TR) is determined by multiplying the likelihood and impact values:

$$TR = L \times I$$

This formula represents the inherent or unmitigated risk level essentially, the risk that exists before any controls or safeguards are considered. For example, a high-likelihood, high-impact ransomware attack (L = 5, I = 5) would yield a Total Risk score of 25, categorising it as an extreme-level risk requiring immediate mitigation (Clark et al., 2025)

The Residual Risk (RR), which is the remaining level of risk after applying mitigation measures, is calculated using the following formula:

$$RR = TR \times (1 - C)$$

In this formula, the Control Effectiveness (C) value is subtracted from 1 to determine the proportion of risk that remains unmitigated. For instance, if an organisation has a control effectiveness score of 0.4 (moderately effective controls), then 60% of the inherent risk remains. Continuing the earlier example, a Total Risk score of 25 with a control effectiveness of 0.4 would result in a Residual Risk of 15.0, indicating a persistent high-risk exposure even after controls have been implemented.

This quantitative framework provides a transparent and repeatable method for risk comparison across multiple systems, departments, or facilities. For instance, risks with similar Total Risk scores may have different Residual Risks depending on how effective their existing controls are. Such differentiation enables NHS management to focus resources on areas where control gaps are most pronounced, rather than where risk levels appear superficially high. The scoring mechanism also supports continuous monitoring allowing risk scores to be recalculated dynamically as new threats emerge or controls are improved.

The NRAST tool also integrates this scoring system into a risk categorisation model, grouping risks into four main tiers based on the calculated Residual Risk (RR) value:

Low Risk (RR ≤ 5): Minimal operational or security impact; routine monitoring sufficient.

Medium Risk (6 ≤ RR ≤ 10): Noticeable impact requiring control reinforcement.

High Risk (11 ≤ RR ≤ 15): Significant potential impact requiring prompt mitigation.

Extreme Risk (RR ≥ 16): Critical threats requiring immediate remediation and executive-level attention.

This classification system allows hospital leadership and security teams to prioritise high and extreme risks, ensuring that limited cybersecurity resources are directed towards the most critical vulnerabilities affecting patient care and operational continuity. By using these well-defined thresholds, the NRAST tool transforms abstract cybersecurity risks into actionable intelligence, improving communication between technical teams and non-technical stakeholders.

Moreover, the tool's methodology is designed to be flexible and auditable, supporting integration with other risk management frameworks such as ISO/IEC 27005, NHS Cyber Assessment Framework, and the GDPR accountability principle (Ibrahim et al., 2018).This ensures that each calculated risk value not only reflects internal security priorities but also contributes to regulatory compliance and strategic planning.

In summary, the NRAST's scoring and weighting system operationalises NIST's theoretical guidance into a practical, quantitative tool for the healthcare sector. By linking the concepts of likelihood, impact, and control effectiveness into measurable outcomes, it empowers NHS organisations to prioritise mitigation strategies, allocate resources effectively, and maintain an ongoing, data-driven understanding of their cybersecurity posture (NCSC, 2024).

# Critical Assessment of the Solution

The NHS Risk Analysis and Scoring Tool (NRAST) developed in this study provides a structured and evidence-based mechanism for assessing cybersecurity risks in healthcare environments. When evaluated against established theoretical and practical criteria from information security risk management literature, the tool demonstrates several strengths, including methodological soundness, adaptability, and alignment with international standards. However, it also presents certain limitations relating to scalability, data subjectivity, and integration challenges, which must be addressed to enhance its real-world applicability.

## Strengths and Theoretical Alignment

From a theoretical standpoint, the NRAST tool strongly aligns with the core principles of the NIST framework (NIST, 2012), which emphasises a cyclical, data-driven approach to risk management:

preparation, assessment, communication, maintenance, and response. The tool effectively operationalises these stages by embedding structured scoring, risk classification, and continuous reassessment processes. This ensures that the tool is not merely descriptive but functions as a dynamic decision-support system, capable of adapting to evolving threat landscapes.

Furthermore, the tool integrates fundamental principles from risk management theory, including the CIA triad, risk quantification, and residual risk measurement (Kör, Taşkın and Metin, 2025). These theoretical constructs are implemented through the use of quantifiable parameters likelihood, impact, and control effectiveness, to calculate total and residual risk scores. The quantification of risk enhances transparency and accountability in cybersecurity governance, allowing NHS decision-makers to prioritise resources effectively.

Another theoretical strength of the NRAST is its interdisciplinary design. It incorporates both technical controls (e.g., encryption, and network segmentation) and organisational factors (e.g., staff training, and incident response), reflecting the holistic nature of modern risk theory (ISO/IEC, 2018). By combining qualitative judgments with quantitative scoring, the tool adheres to hybrid risk assessment methodologies recommended by the International Organization for Standardization and NIST, bridging the gap between subjective expert evaluation and empirical data (ISO/IEC, 2018).

Finally, the tool's structured risk register and visual analytics components align with NHS Digital's Cyber Assessment Framework , which prioritises continuous monitoring and data-driven decision-making in critical healthcare systems (NHS Digital, 2023). The integration of residual risk tracking and control effectiveness monitoring further supports the theoretical requirement for feedback loops within risk management systems.

## Shortcomings and Limitations

Despite its strong theoretical foundation, the NRAST tool faces several limitations that could affect its precision, scalability, and ease of use in large or complex healthcare environments.

Firstly, the subjectivity of scoring inputs presents a challenge. While the tool relies on expert judgment to assign likelihood and impact values, these assessments can vary significantly between assessors due to differences in experience, perception of risk, or understanding of threats. Such variability may lead to inconsistencies in the final risk scores, potentially distorting risk prioritisation (NCSC, 2024). Implementing standardised calibration workshops or baseline scoring guidelines could mitigate this issue by ensuring greater uniformity across users.

Secondly, the tool's current version is manual and semi-automated, requiring assessors to input data and interpret results without the aid of machine learning or real-time analytics. This limits scalability and responsiveness, particularly for large NHS networks comprising multiple hospitals and departments. A more advanced, automated version could integrate data feeds from security information and event management (SIEM) systems and vulnerability scanners to generate real-time risk dashboards (Mohamed Mohideen et al., 2024)

Thirdly, while the tool is designed around NIST, it does not fully incorporate the financial or economic dimension of risk, which frameworks such as FAIR (Factor Analysis of Information Risk) provide. Without quantifying risk in monetary terms, NHS decision-makers may find it difficult to compare cybersecurity investments against operational costs or patient service priorities. Incorporating cost-benefit analysis modules would significantly improve decision-making and justify resource allocation (Srivastava et al., 2024).

Another limitation concerns data integration and interoperability. The NHS employs a range of legacy systems and third-party platforms, many of which operate on incompatible architectures. Integrating NRAST outputs with existing NHS Digital tools, compliance platforms, or Electronic Health Record (EHR) systems may require additional technical customisation.

Finally, while the tool performs well at identifying and ranking cyber risks, it does not yet include a predictive or adaptive risk modelling component. The inclusion of threat intelligence data, predictive analytics, or AI-driven anomaly detection could transform NRAST from a reactive tool into a proactive cybersecurity management platform capable of anticipating threats before they materialise.

## Opportunities for Improvement

To overcome these limitations, several enhancements can be implemented.

**Automation and Integration**: Developing NRAST as a web-based or cloud-enabled platform would allow real-time integration with NHS monitoring systems, automating data collection and risk calculation. This would significantly reduce manual input errors and enhance scalability.

**Incorporation of FAIR and Cost Analysis**: By combining NIST's qualitative model with the quantitative cost-based approach of FAIR, future iterations could include monetary value estimations for each risk, aiding financial decision-making and budget justification (Hubbard and Seiersen, 2016).

**Enhanced Data Validation**: Standardising risk scoring through calibration sessions or automated questionnaires can reduce assessor bias and improve consistency.

**Predictive Analytics**: Integration of AI and machine learning could enable trend analysis, identifying emerging threats and dynamically adjusting risk scores based on behavioural patterns.

**User Interface and Accessibility**: Developing an intuitive dashboard with visual aids such as heat maps, graphs, and trend lines can enhance understanding and facilitate decision-making for both technical and non-technical stakeholders.

## Practical Adaptation in Real-World Healthcare Settings

The NRAST tool is highly adaptable to real-world implementation within the NHS and similar healthcare environments. Its modular architecture allows it to be customised according to organisational size, digital maturity, and regulatory requirements. For smaller hospitals or clinics, the tool can be deployed as a spreadsheet-based risk tracker integrated with basic assessment forms. For larger healthcare networks, a web-based platform can be developed, incorporating centralised databases, risk dashboards, and automated reporting features.

Moreover, the tool's design aligns with key regulatory frameworks such as the GDPR, NHS Cyber Assessment Frameworkand NCSC risk management guidance, ensuring compliance and audit readiness (Tharun et al., 2025). Its structured documentation of residual risks and countermeasures also facilitates easier reporting to oversight bodies and executive boards.

In addition, the NRAST tool can serve as a training and governance instrument, helping hospital IT staff and managers build a culture of risk awareness. Through regular use, it can improve communication between technical teams and executive leadership, ensuring that cybersecurity is managed as a business priority rather than solely an IT concern.

# Conclusion

This report conducted a comprehensive risk analysis of the 2024 NHS cyber attack using the NIST risk assessment methodology. The analysis demonstrated that healthcare organisations such as the NHS face increasingly complex cyber threats including ransomware, vendor breaches, insider misuse, and data loss that directly endanger patient safety and operational continuity. To address these challenges, the NHS Risk Analysis and Scoring Tool was developed as a structured, data-driven mechanism for identifying, evaluating, and prioritising risks.

The findings revealed that the NHS's major vulnerabilities stem from inadequate patch management, weak third-party controls, insufficient network segmentation, and inconsistent incident response preparedness. The NRAST tool quantified these weaknesses using weighted parameters for likelihood, impact, and control effectiveness, allowing for clear visibility of both total and residual risks. This enabled the ranking of risks from low to extreme severity and the formulation of targeted countermeasures.

The report recommends the implementation of a multi-layered mitigation strategy that includes multi-factor authentication, automated patch management, network segmentation, security operations centre integration, and offline immutable backups to strengthen cyber resilience. It also emphasises the need for continuous monitoring, regular staff training, and vendor security audits to maintain compliance with GDPR and NHS Cyber Assessment Framework requirements.

Overall, the study concludes that adopting the NIST methodology supported by the NRAST tool provides an effective, repeatable, and transparent approach for managing cyber risks in healthcare. When embedded within NHS operations, this framework can significantly improve decision-making, reduce incident response times, and protect critical healthcare systems from future attacks, thereby ensuring the confidentiality, integrity, and availability of patient data and services.

# References


1. Abdi, A., Bennouri, H. and Keane, A. (2024) 'Emerging cyber risks & threats in healthcare systems: a case study in resilient cybersecurity solutions', 2024 13th Mediterranean Conference on Embedded Computing (MECO 2024). IEEE. Available at: https://doi.org/10.1109/MECO62516.2024.10577790 (Accessed: 6 October 2025).
2. Bernardo, L., Malta, S. and Magalhães, J. (2025) 'An evaluation framework for cybersecurity maturity aligned with the NIST CSF', Electronics (Switzerland), 14(7), Article no. 1364. Available at: https://doi.org/10.3390/electronics14071364 (Accessed: 6 October 2025).
3. Calvo, A., Escuder, S., Ortiz, N., Escrig, J. and Compastié, M. (2025) 'RBD24: A labelled dataset with risk activities using log application data', *Computers and Security*, 150, Article no. 104290. Available at: https://doi.org/10.1016/j.cose.2024.104290 (Accessed: 6 October 2025)
4. Clark, C., Berry, H.S., Sullivan, B., Maroney, N. and Galbraith, J. (2025) 'Malware exploitation and vulnerability assessment of CVE-2024-38063 in Windows 10 and 11 in academic networks cybersecurity', ISDFS 2025 - 13th International Symposium on Digital Forensics and Security. IEEE. Available at: https://doi.org/10.1109/ISDFS65363.2025.11011991 (Accessed: 6 October 2025).
5. Ibrahim, A., Valli, C., McAteer, I. and Chaudhry, J. (2018) 'A security review of local government using NIST CSF: a case study', Journal of Supercomputing, 74(10), pp. 5171–5186. Available at: https://doi.org/10.1007/s11227-018-2479-2 (Accessed: 6 October 2025).

6. Kör, B., Taşkın, N. and Metin, B. (2025) ‘Perceptions of digitalisation and cyber security: impacts on organisational practices through the NIST Cybersecurity Framework’, Journal of Decision Systems, 34(1), Article no. 2522848. Available at: https://doi.org/10.1080/12460125.2025.2522848 (Accessed: 6 October 2025).
7. Meshkat, L. and Miller, R.L. (2022) ‘Quantifying cybersecurity risk for NASA missions’, Proceedings - Annual Reliability and Maintainability Symposium, 2022-January. IEEE. Available at: https://doi.org/10.1109/RAMS51457.2022.9893983 (Accessed: 6 October 2025).
8. Mohamed Mohideen, M.A. et al. (2024) ‘Behind the code: identifying zero-day exploits in WordPress’, Future Internet, 16(7), Article no. 256. Available at: https://doi.org/10.3390/fi16070256 (Accessed: 6 October 2025)
9. Srivastava, K. et al. (2024) ‘Assessment of the impact of cyber-attacks and security breaches in diagnostic systems on the healthcare sector’, 2024 IEEE International Conference on Cyber Security and Resilience (CSR 2024), pp. 531–536. Available at: https://doi.org/10.1109/CSR61664.2024.10679475 (Accessed: 6 October 2025).
10. Tharun, P. et al. (2025) ‘Convolutional neural network for advanced intrusion detection for data balancing on system efficiency’, Proceedings of 8th International Conference on Computing Methodologies and Communication (ICCMC 2025), pp. 145–152. Available at: https://doi.org/10.1109/ICCMC65190.2025.11140907 (Accessed: 6 October 2025).