GIS Odyssey Journal

2025 • Volume 5 • Number 1

https://doi.org/10.57599/gisoj.2025.5.1.59

Maciej Kiedrowicz[1]

# GIS SECURITY INCIDENT MANAGEMENT: PRACTICAL APPROACHES AND STANDARDS

**Abstract:** In the face of growing cyber threats, security incident management in GIS (Geographic Information Systems) systems is becoming a key element in ensuring the integrity and availability of spatial data. The aim of this article is to analyze practical approaches to security incident management in GIS systems and to assess compliance with international standards. The study used real-life incident case analysis methods, a literature review and interviews with industry experts. The results point to the need for integrated incident management procedures that include monitoring, detection, response and incident reporting. In addition, compliance with ISO 27001, ISO 19115 and OGC (Open Geospatial Consortium) standards is crucial for effective spatial data security management. The article ends with recommendations for the implementation of best practices and proposals for further research in the area of security incident management in GIS systems.

**Keywords:** Incident management, Cybersecurity, GIS systems, Compliance standards, Cyber threats

Received: 3 March 2025; accepted: 25 March 2025



[1] Military University of Technology, Faculty of Cybernetics, Warsaw, Poland, ORCID ID: https://orcid.org/0000-0002-4389-0774, email: maciej.kiedrowicz@wat.edu.pl

## Introduction

Geographic information systems (GIS) play a key role in many fields, such as spatial planning, natural resource management, logistics, and incident management (ISO–ArcGIS, 2025). Cybersecurity incident management is the process of identifying, analyzing, responding to, and restoring normal operations after information security incidents. These incidents can include hacking attacks, data breaches, malware, phishing, and other cyber threats.

With the ability to integrate and analyze spatial data, GIS enables more informed decisions and a better understanding of complex spatial relationships. However, as GIS becomes increasingly important, so do the risks associated with cyber threats. Attacks on GIS systems can lead to data loss, disruption to critical infrastructure, and serious consequences for public safety (Singh, 2024; Tomaszewski et al., 2015; Wei, 2021).

Despite the growing number of studies on security incident management in information systems, specific aspects related to GIS are relatively rarely discussed. There is a need for more detailed research on methods of detecting, responding and reporting incidents in the context of spatial data. In addition, there is a lack of research on the compliance of GIS systems with international security standards, such as ISO 27001 and OGC.

Despite the growing body of research on GIS security incident management, there is a limited amount of literature that examines in detail the effectiveness of different standards and practical approaches in the context of specific industry requirements. In particular, there is a lack of empirical research that evaluates how standards such as DORA, NIS2, NIST, and ISO 27001 affect incident management in GIS systems in various industry sectors. In addition, there are few studies that examine the integration of these standards into existing GIS incident management procedures and their impact on improving the cyber resilience of organizations.

The main research problem is to identify effective methods of managing security incidents in GIS systems and to assess their compliance with international standards. In particular, the study focuses on the analysis of incident detection, response and reporting procedures and on the assessment of the extent to which these procedures comply with the applicable norms and standards.

Therefore, the main research questions that will be analyzed in the article are:

1. What are the main security risks specific to GIS?
2. What are the most common security incidents in GIS systems and what are their causes?
3. What incident management standards are currently used in GIS systems and how are they implemented?
4. What are the best practices in managing security incidents in GIS systems that can be adapted from other fields of computer science?
5. What methods of incident detection, response, and reporting are used in GIS systems?
6. To what extent are GIS systems compliant with international security standards such as ISO 27001 and OGC?
7. What recommendations can be made to improve GIS security incident management?

The aim of this article is to analyze practical approaches to security incident management in GIS systems and to assess compliance with international standards. Security incident management is crucial to ensure the integrity, confidentiality, and availability of spatial data, which has a direct impact on the efficiency and reliability of GIS systems (FEMA, 2025; NIST, 2012). The article will present methods of detecting, responding to and reporting incidents, as well as discuss standards such as ISO 27001 and OGC, which support information security management in the context of GIS (DeMers, 2008; FEMA, 2025; NIST, 2012).

The article begins with an "Introduction" that discusses the background, research gap, research problem, and research questions that focus on security incident management in GIS. The "Literature review" chapter examines existing research and publications on GIS security incident management. The next chapter is "Methodology", which provides a detailed description of the research approach used to investigate effective practical approaches and standards for managing security incidents in GIS. The "Results" chapter outlines key security risks in GIS, an assessment of the effectiveness of various incident management standards, and best practices. The "Conclusions and recommendations" summarize the main results and propose practical recommendations and directions for future research.

## Literature review

The literature on books that describe effective and practical approaches and standards for managing security incidents in GIS systems is rich and diverse. Key books include titles such as:

"Geographic Information Systems (GIS) for Disaster Management" by Brian Tomaszewski, which offers a comprehensive overview of the use of GIS in disaster management, including security incident management. It includes hands-on exercises and case studies that show how GIS can be used at different stages of disaster management.

"Dealing with Disasters: GIS for Emergency Management" by Ryan Lanclos and Matt Artz presents a modern approach to managing threats and disasters with GIS. The book includes case studies from various emergency management agencies that effectively use GIS for risk analysis, situational awareness, and response and recovery management.

"Geographical Information Systems: A Practical Approach" by Xuan Zhu combines GIS theory with practice, helping readers understand key GIS concepts and methods. It includes updated case studies that illustrate innovative applications of GIS in a variety of fields, including security incident management.

These books provide a solid understanding of GIS security incident management and practical approaches and standards that can be applied to minimize the risk and impact of incidents.

Contemporary scientific articles and journals provide up-to-date information on the development of GIS technology and security incident management. The journal Advances in Geodesy and Geoinformation publishes peer-reviewed articles on geodesy, geoinformation, cartography, and GIS, including research on spatial data management and

security. Google Scholar is also a valuable resource, enabling extensive searches of scientific literature in various fields, including GIS. Scientific articles often focus on new methods of spatial data analysis, applications of artificial intelligence, and challenges related to cybersecurity in the context of GIS (Werner, 2018).

Domain and specialist reports provide detailed analyses and recommendations for managing security incidents in GIS systems. An example is the "Geostatistics Portal – GIS as a source of information about territory and society", which discusses the applications of GIS in official statistics and spatial analyses (Simpson, 2024). These reports often include data from real-life cases, risk analyses, and suggestions for best practices in spatial data security management (ESRI, 2025; Lanclos & Artz, 2021).

## Methodology

This study uses a multifaceted approach to the analysis of security incidents in GIS systems. A combination of qualitative and quantitative methods was used to obtain a more complete picture of the problem. The following methods were used for incident analysis (Table 1).

Table 1. List of methods for the analysis of security incidents in GIS systems

| Method name | Scope of activities |
|---|---|
| Thematic method | This method involves identifying and analyzing the main themes and patterns that appear in security incident data. Coding techniques were used to isolate key topics and understand their importance in the context of incident management (IPCC, 2025). |
| Interviews with experts | Information security experts and GIS specialists were interviewed to gain their perspective on security incident management. These interviews provided valuable information on practical challenges and best practices in the field (UNDRR, 2025). |
| Log analysis & monitoring | Tools for analyzing system logs and monitoring network activity, such as SIEM (Security Information and Event Management), were used. These tools made it possible to detect anomalies and suspicious activities in real time (Zhu, 2016; USGS, 2025). |
| Analysis of professional and specialist literature | An in-depth analysis of the professional and specialist literature was conducted to identify existing research and publications on GIS security incident management. This analysis allowed us to understand current trends, challenges and best practices in this field. |

Source: Own study

The study used a variety of data sources to provide a comprehensive analysis of security incidents in GIS systems. These sources are included in Table 2.

## Results

GIS systems, like other IT systems, are exposed to a variety of security incidents. The most common incidents include Table 3.

Managing security incidents in GIS systems requires the implementation of standard procedures and protocols that ensure effective incident detection, response, and reporting. Standard Operating Procedures (SOPs) are critical to maintaining consistency and efficiency. These procedures include several key steps: incident identification, impact assessment, incident response, recovery and post-incident analysis. Incident identification involves detecting unauthorized activities or anomalies in the GIS using monitoring tools.

Table 2. List of data sources

| Source | Scope of activities |
|---|---|
| Incident reports | Security incident reports reported by organizations using GIS systems were analyzed. These reports contained detailed information on the nature of the incidents, their causes, and the corrective actions taken (Simpson, 2024). |
| Survey | Surveys were conducted among GIS users to collect data on their experience with security incidents and their incident management procedures. |
| Interviews | As mentioned earlier, interviews with experts provided additional information on the practical aspects of security incident management in GIS systems (UNDRR, 2025). |
| Data from monitoring tools | It used data from monitoring tools such as SIEM to analyze network activity and detect anomalies. This data allowed for the identification of patterns of behavior related to security incidents (Zhu, 2016). |
| Professional and specialist literature | The literature analysis included a review of scientific articles, industry reports, and technical documentation on security incident management in GIS systems. |

Source: Own study

Table 3. List of the most common incidents with examples

| Incident type | Effects | Examples of real-world incidents |
|---|---|---|
| Unauthorized access | A security breach where GIS or spatial data is accessed without proper permissions. This can lead to data theft, modification or deletion (CISA, 2023; NIST, 2012). | In 2023, the company experienced an incident where an unauthorized user gained access to the GIS and copied sensitive critical infrastructure data. The cause of the incident was a weak password policy and the lack of two-factor authentication. The incident resulted in the need to conduct a costly forensic analysis and introduce new security procedures (EEA, 2024). |
| Ransomware attacks | The criminals use malware to encrypt GIS data and demand a ransom to unlock it. These types of attacks can seriously disrupt GIS systems and lead to the loss of critical data (CISA, 2023; NIST, 2012). | In 2024, the city hall fell victim to a ransomware attack that resulted in the encryption of GIS spatial planning data. The attackers demanded a ransom in cryptocurrencies to unlock the data. The cause of the incident was a vulnerability in the system that allowed the introduction of malware. The incident resulted in the loss of access to data for several days and the need to pay a ransom (UNDRR, 2025). |
| Phishing | A method of impersonating trusted entities to obtain sensitive information, such as GIS passwords. Successful phishing attacks can enable unauthorized access to systems (CISA, 2023; NIST, 2012). | In 2022, the company experienced a phishing attack that resulted in an employee exposing their GIS login credentials. The attackers used this data to gain unauthorized access to the system and modify spatial data. The cause of the incident was insufficient education of employees about the dangers of phishing. The incident resulted in the need to restore data from backups and conduct security training (UNDRR, 2025). |
| DDoS (Distributed Denial of Service) attacks | Attacks that overwhelm a GIS server or network with an excess of fraudulent requests, leading to unavailability of services for users (CISA, 2023; NIST, 2012). | |
| Human errors | Incidents resulting from mistakes made by GIS users, such as accidental deletion of data, improper system configurations, or failure to follow security procedures (CISA, 2023) (NIST, 2012). | |

Source: Own study

An incident impact assessment includes an analysis of the potential impact on data and systems. Incident response includes actions to limit damage, such as isolating infected systems or blocking unauthorized access. Restoring normal operations involves repairing damaged systems and data and putting in place preventive measures. Post-incident analysis aims to identify the causes of the incident and implement preventive measures to avoid similar situations in the future (Tomaszewski, 2020).

Tools and technologies supporting these processes play a key role in managing security incidents in GIS systems. Surveillance systems such as SIEM (Security Information and Event Management) enable continuous monitoring of network activity and detection of anomalies in real-time. Log analysis software such as Splunk or ELK Stack allows you to collect, analyze, and correlate data from various sources, making it easier to identify and analyze incidents. Incident management tools such as ServiceNow or JIRA support incident management processes by allowing you to track tickets, coordinate activities, and document incidents and actions taken. Additionally, technologies such as artificial intelligence and machine learning can be used to automatically detect patterns and anomalies in data, which increases the effectiveness of incident detection (HAZUS, 2025; FEMA, 2025; NIST, 2012).

The set of best practices in cybersecurity incident management includes:

1. Developing incident response plans – clear procedures and policies for incident response.
2. Regular training and exercises – training teams and conducting incident simulations.
3. Monitoring and analysis – continuous monitoring of IT systems and analysis of security events.
4. Process automation – the use of tools to automate incident detection and response.
5. Cross-team collaboration – close collaboration between IT, security, and risk management teams.
6. Documentation and reporting – detailed documentation of incidents and reporting to management.

In the context of GIS security incident management, international standards such as ISO 27001, ISO 19115 and standards developed by the Open Geospatial Consortium (OGC) are of key importance. ISO 27001 is an international standard for information security management that promotes a holistic approach to data protection, including people, policies, and technology (ISO–ArcGIS, 2025). This standard is particularly relevant for GIS systems because it provides a framework for managing risk and protecting spatial data from unauthorized access and other threats.

ISO 19115 is a geographic metadata standard that defines a framework for describing geographic information and services using metadata (ISO, 2014). This standard is crucial for GIS systems because it enables accurate and consistent documentation of spatial data, which is essential for its effective management and exchange. ISO 19115 covers information on the identification, scope, quality, spatial and temporal aspects, content, spatial references, and other properties of geographic data.

The Open Geospatial Consortium (OGC) develops and maintains international standards for geographic content and location-based services. OGC standards such as

Web Map Service (WMS), Web Feature Service (WFS), and Web Coverage Service (WCS) enable interoperability between different GIS systems, allowing for seamless exchange and integration of spatial data. These standards are widely used in the geoinformation industry and support the development of innovative solutions based on spatial data.

Managing security incidents in GIS also requires compliance with various legal and regulatory requirements. In the European Union, the NIS2 (Network and Information Systems Directive) imposes obligations on operators of essential services, including GIS systems, regarding the management of security risks and incidents (CISA, 2023; Simpson, 2024). This Directive requires the implementation of appropriate technical and organisational measures to ensure the security of network and information systems and to report serious incidents to the relevant supervisory authorities.

In addition, compliance with data protection regulations such as the GDPR (General Data Protection Regulation) is crucial for GIS systems that process personal data. The GDPR requires organizations to implement appropriate data protection measures, such as pseudonymization and encryption, and ensure data subject rights, such as the right to access and delete data (CISA, 2024).

## Conclusions and recommendations

Cybersecurity incident management is a key component of an organization's security strategy, ensuring effective response to threats and minimizing their impact on business operations. Effective implementation of incident management requires a comprehensive approach that combines technologies, processes, and employee education.

Analysis of security incidents in GIS systems has shown that the most common incidents include unauthorized access, ransomware attacks, phishing, DDoS attacks, and human error. Real-world incidents highlight the importance of effective incident management procedures and the need for appropriate monitoring tools and technologies. The use of international standards such as ISO 27001, ISO 19115 and OGC standards is crucial to ensure the security of spatial data and the interoperability of GIS systems. Compliance with legal regulations such as the NIS2 directive and the GDPR is essential for data protection and risk management.

To improve security incident management in GIS, it is recommended to implement integrated incident management procedures that include identification, assessment, response, recovery and post-incident analysis. Organizations should invest in advanced monitoring tools, such as SIEM, and log analysis software to effectively detect and respond to incidents. It is also important to conduct regular training for employees on information security and to raise awareness of threats such as phishing. Organizations should strive to comply with international security standards and legal regulations to ensure the protection of spatial data and minimize the risk of incidents.

Future research in the area of GIS security incident management should focus on developing new methods for detecting and responding to incidents using artificial intelligence and machine learning. It is also important to study the effectiveness of different monitoring tools and technologies and their impact on incident management.

Further research should also include risk analysis and assessment of the impact of incidents on various sectors, such as critical infrastructure, crisis management or spatial planning. Finally, research should explore opportunities to improve the interoperability of GIS systems by developing and implementing new standards and protocols.

**Acknowledgements**

This work was financed/co-financed by Military University of Technology under research project UGB 531-000023-W500-22.

**References**

CISA (2023). Geographic Information System Lifecycle Best Practices Guide, CISA. https://www.cisa.gov/sites/default/files/2023-02/20_0922_SAFECOM-NCSWIC_GIS_Lifecycle_Best_Practices_Guide_FINAL_508c.pdf [access: 16.01.2025].

CISA (2024). Cybersecurity and Infrastructure Security Agency Annual Report, CISA. https://www.cisa.gov/sites/default/files/2024-12/CSAC%20Annual%20Report_20241210.pdf [access: 16.01.2025].

DeMers M.N. (2008). Fundamentals of Geographic Information Systems. Wiley. 4th edition.

FEMA (2025). The Federal Emergency Management Agency (FEMA), National Incident Management System (NIMS), Department of Homeland Security, https://www.fema.gov/emergency-managers/nims [access: 16.01.2025].

EEA Report (2024). European Environment Agency – Trends and projections in Europe 2024. DOI:10.2800/7574066

ESRI (2025). What is GIS? Geographic Information System (GIS), Esri. https://www.esri.com/pl-pl/what-is-gis/overview [access: 06.02.2025].

ISO–ArcGIS (2025). ISO–ArcGIS Trust Center, Documentation. https://trust.arcgis.com/en/compliance/iso-information.htm [access: 11.01.2025].

HAZUS (2025). FEMA's Hazus Program – GIS-Based Software for Estimating Potential Losses from Disasters, Federal Emergency Management Agency. https://www.fema.gov/flood-maps/products-tools/hazus [access: 11.01.2025].

IPCC (2025). Intergovernmental Panel on Climate Change Assessment Reports, IPCC. https://www.ipcc.ch/assessment-report/ar6/ [access: 11.01.2025].

ISO (2014). ISO 19115-1:2014 – Geographic information – Metadata Part 1: Fundamentals, ISO. https://www.iso.org/standard/53798.html [access: 11.01.2025].

Simpson C. (2024). JRC Highlights Report 2023. In: I. Bonjean, M. Fornara, K. Jonkers, T. Klaassen, S. Lehto, L. Soldatova, J. Thielen Del Pozo, M. Westra Van Holthe (ed.), Publications Office of the European Union, Luxembourg. JRC136884. doi:10.2760/947345.

Lanclos R., Artz M. (2021). Dealing with Disasters: GIS for Emergency Management. Esri Press.

NIST (2012). NIST Special Publication 800-61 Revision 2: Computer Security Incident Handling Guide. P. Cichonski, T. Millar, T. Grance, K. Scarfone (recommendations). http://dx.doi.org/10.6028/NIST.SP.800-61r2.

Singh R. (2024) The role of geographic information systems (GIS) in disaster management and planning. International Journal of Geography, Geology and Environment, vol. 6, no. 2, pp. 195–205. DOI: 10.22271/27067483.2024.v6.i2c.305.

Tomaszewski B., Judex M., Szarzynski J., Radestock C. Wirkus L. (2015). Geographic Information Systems for Disaster Response: A Review. Journal of Homeland Security and Emergency Management, vol. 12, no. 3, pp. 571–602. https://doi.org/10.1515/jhsem-2014-0082.

Tomaszewski B. (2020). Geographic Information Systems (GIS) for Disaster Management. 2nd ed. Taylor and Francis. https://www.perlego.com/book/1899960/geographic-information-systems-gis-for-disaster-management-pdf [access: 15 January 2025].

UNDRR (2025). United Nations Office for Disaster Risk Reduction, Global Assessment Report on Disaster Risk Reduction. https://www.undrr.org/gar [access: 15.01.2025].

USGS (2025). United States Geological Survey Annual Reports, USGS. https://www.usgs.gov [access: 15.01.2025].

Wei H.L. (2021). Geographic Information Systems (GIS) Applications in Emergency Management. In: L.R. Shapiro, M.H. Maras, (ed.), Encyclopedia of Security and Emergency Management. Springer, Cham. https://doi.org/10.1007/978-3-319-70488-3_13.

Werner P. (2018). Czy GIS podnosi rangę dyscyplin geograficznych? Znaczenie GIS i GIScience dla geografii (*Does GIS raise the profile of geographical disciplines? The importance of GIS and GIScience for geography*). Acta Universitatis Lodziensis, no. 34. DOI: https://doi.org/10.18778/1508-1117.34.01.

Zhu X. (2016). GIS for Environmental Applications: A practical approach, 1st ed. Routledge. https://doi.org/10.4324/9780203383124.