NBP. Nauka, bezbednost, policija
Published by
University of Criminal Investigation and Police Studies
2026, Vol. 31, Issue 3, pp.
https://doi.org/10.5937/nabepo31-61549
Review Essay

Insider Threats in the Context of Information Security: Risks, Challenges and Protection Strategies

Goran Matić[1]

Office of the National Security Council and Classified Information Protection, Belgrade, Serbia

Submitted: 2025-09-17 • Accepted: 2025-12-24 • Published: 2026-03-30

Abstract: Insider threats represent a critical challenge to information security, stemming from individuals with authorized access who may compromise data integrity through malicious or negligent actions. This study employs a multidisciplinary approach – integrating literature review, case studies, and legal analysis – to examine the nature, drivers, and mitigation strategies for insider threats. It compares whistleblowing, privilege abuse, espionage, and sabotage across legal, psychological, and organizational dimensions. A key finding is the blurred line between whistleblowers acting in the public interest and harmful insiders, underscoring the need for clear legal criteria. The analysis reveals that weak employee protections and toxic work environments increase retaliatory risks. The paper concludes with recommendations for a holistic defence strategy combining technical controls, legal frameworks, and organizational culture, with specific proposals for improving Serbia's fragmented regulatory system.

Keywords: insider threat, information security, whistleblowing, legal framework, organizational culture.

INTRODUCTION

Insider threats are among the most complex challenges in modern information security. Unlike external attackers, insiders possess legitimate access to systems and data, making their actions difficult to detect (Cybersecurity and Infrastructure Security Agency, 2024). An insider is defined as any individual – employee, contractor, or consultant – with authorized access who may misuse it intentionally or unintentionally (Singh & Sharma, 2022). According to CISA, an insider threat is the risk that such a person could cause harm to systems, data, personnel, or assets. The ambiguity surrounding this term complicates prevention, especially when overlapping with issues like whistleblowing, harassment, or freedom of expression (Gheyas & Abdallah, 2016).

1 Corresponding author: goran.matic@nsa.gov.rs • office@nsa.gov.rs • https://orcid.org/0000-0001-8443-5797

eISSN 2620-0406

Information security, as defined by International Organization for Standardization & International Electrotechnical Commission – ISO/IEC 27000 (International Organization for Standardization [ISO], 2018), refers to the preservation of confidentiality, integrity, and availability of information, achieved through technical, organizational, and human measures. Protecting information in both physical and digital formats is essential for organizational continuity. However, safeguarding assets must be balanced with the protection of fundamental rights, including privacy and freedom of expression. This balance is not merely a technical or administrative concern; it is a foundational principle of democratic governance, where the state's duty to secure its institutions must not override the individual's right to speak truth to power. The tension between these two imperatives becomes especially visible in contexts where institutional trust is weak, legal frameworks are underdeveloped, and accountability mechanisms are either absent or selectively enforced.

In Serbia, cases such as Aleksandar Obradović at Krušik and Momčilo Perišić highlight this tension. Obradović exposed alleged corruption but faced prosecution, raising questions about whether his act was whistleblowing or a security breach (Jeremić, 2024). His actions, while disruptive to institutional hierarchies, were motivated by a desire to reveal financial misconduct that he believed undermined national interests. Yet, rather than being recognized as a protector of public accountability, he was treated as a violator of security protocols – a criminal rather than a civic actor. Similarly, Perišić was convicted of espionage after sharing military secrets with a foreign embassy (Derikonjić, 2023) His case, like Obradović's, was adjudicated not on the basis of intent or public interest, but solely on the fact of unauthorized transmission – a legal reductionism that ignores the moral complexity of the act. These cases illustrate the urgent need for legal clarity in differentiating public-interest disclosures from harmful insider acts. Without such clarity, institutions risk criminalising dissent, deterring ethical behaviour, and reinforcing cultures of silence that ultimately make them more vulnerable.

This paper addresses the following research questions: what are the primary causes of insider threats? How do psychological and sociological factors influence insider behaviour? Which strategies are most effective for prevention? And how do legal frameworks regulate these threats, particularly in Serbia? To answer them, the study adopts a multidisciplinary lens, integrating technical, legal, and organizational perspectives. It does not seek to propose new technologies or invent new legal categories. Instead, it seeks to deepen the understanding of what is already present: the existing definitions, the documented cases, the established laws, and the recognized patterns of behaviour. It asks not what should be done, but what is already implied – and why it remains unaddressed.

The insider threat is not simply a problem of access control or data leakage. It is a problem of trust – and of the breakdown of trust. When individuals who are entrusted with institutional knowledge feel that their concerns are ignored, their integrity is questioned, or their loyalty is exploited, their relationship with the organization shifts from one of cooperation to one of alienation. In such environments, even well-intentioned employees may come to see information as a weapon – not because they are malicious, but because they believe the system has already weaponised silence. This transformation is not sudden; it is gradual, cumulative, and often invisible until it manifests in a leak, a sabotage, or a resignation.

The challenge, then, is not merely to detect insiders who act wrongly, but to understand why so many who might act rightly are instead driven to the margins – or to the dark.

THEORETICAL FRAMEWORK FOR STUDYING INSIDER THREATS

Insider threats can be categorized into three types: malicious, negligent, and infiltrators (Schoenherr et al., 2022). Malicious insiders deliberately steal data or sabotage systems; negligent insiders unintentionally compromise security through errors; infiltrators are external actors who gain access via social engineering. Each category reflects a different dynamic – one of intent, one of oversight, and one of deception – yet all three share a common vulnerability: the assumption that authorized access equates to authorized intent. This assumption is the foundation of most security protocols, and it is also their greatest weakness.

Psychological drivers include dissatisfaction, financial pressure, revenge, or ideology (Ruohonen & Saddiqa, 2024). These are not random impulses; they are responses to perceived conditions – conditions of unfairness, neglect, or betrayal. A malicious insider does not emerge from a vacuum. They emerge from an environment where grievances have been ignored, where promotions have been denied without explanation, where ethical concerns have been met with silence, and where the organization has failed to provide a legitimate channel for redress. Financial pressure may be the immediate trigger, but it is rarely the root cause. The deeper cause is often a sense of disenfranchisement – the belief that one's voice does not matter, that one's contributions are invisible, and that the system is designed to protect itself, not those who serve it.

Sociological factors – such as corporate culture, oversight quality, and policy clarity – also significantly shape risk levels (Alsowail & Al-Shehari 2021). A toxic culture of fear, where speaking up is equated with disloyalty, creates fertile ground for insider threats. When leadership communicates through top-down directives rather than open dialogue, when audits are conducted as punitive exercises rather than learning opportunities, and when reporting mechanisms are opaque or inaccessible, the organization inadvertently signals that silence is safer than truth. In such environments, even a negligent insider – someone who simply clicks a malicious link or misconfigures a server – may be the product not of carelessness, but of disengagement.

A critical distinction exists between whistleblowers and harmful insiders. Whistleblowers disclose wrongdoing in the public interest and are protected under Article 10 of the European Convention on Human Rights (Council of Europe, 2024), provided their actions are proportionate and necessary. In contrast, espionage involves transferring sensitive information to foreign entities and carries criminal penalties (Warner, 2014). The legal and moral boundaries between these two are not always clear, but they are not arbitrary. The distinction lies in intent, in context, and in the mechanism of disclosure. A whistleblower acts to correct, not to exploit. They act to inform, not to harm. They act within a framework of accountability, even if that framework is imperfect.

Cases like Chelsea Manning and Edward Snowden exemplify the moral ambiguity of such disclosures (Greenwald, 2014; Delmas, 2015). Both individuals accessed classified information under legitimate authority. Both chose to disclose it publicly, bypassing internal channels. Both were labelled as traitors by some and heroes by others. But their actions were not identical to those of a malicious insider who sells data for profit or a foreign agent who infiltrates for strategic gain. Manning and Snowden acted out of conscience, not greed. Their disclosures were selective, not indiscriminate. They sought to spark public debate, not to enable foreign interference.

Yet, under current legal frameworks – including those in Serbia – their actions would likely be treated the same as those of a spy. The law does not distinguish motive. It does not weigh intent. It sees only access and disclosure. This legal rigidity is not neutral; it is profoundly consequential. It discourages ethical behaviour. It punishes accountability. It transforms civic courage into criminal liability.

The failure to distinguish between these categories is not an oversight – it is a feature of systems that prioritize control over transparency.

SECURITY PERSPECTIVE AND ORGANIZATIONAL CULTURE

While technical and legal aspects are often emphasized, the security dimension must be explicitly addressed. Insider threat programs should integrate principles from national frameworks such as the US National Institute of Standard and Technology (NIST) SP 800-53 (National Institute of Standards and Technology [NIST], 2024) and the UK National Protective Security Authority (National Protective Security Authority [NPSA], 2025) guidelines, which advocate for continuous monitoring, access control, and incident response protocols). These frameworks provide valuable structure – they define roles, establish procedures, and outline technical controls. But they remain incomplete without a deeper understanding of the human context in which they operate.

Equally vital is "security culture" – a shared set of values, behaviours, and attitudes that prioritize information protection. Organizations with strong security cultures exhibit lower insider incident rates due to open communication, trust, and employee engagement (Intelligence and National Security Alliance, 2022). Security culture is not a policy document. It is not a training module. It is not a checklist. It is the collective belief that protecting information is everyone's responsibility – not because they are being watched, but because they care.

Cultivating such a culture requires leadership commitment, regular training, and mechanisms for anonymous reporting. Leadership must not only endorse security policies – they must embody them. When executives speak openly about past mistakes, when managers acknowledge their own lapses, when whistleblowers are not punished but listened to, the organization sends a powerful message: that security is not about control, but about integrity.

Training must go beyond compliance. It must engage employees in critical thinking: what does it mean to protect data? When is disclosure justified? What are the consequences of silence? These are not technical questions – they are ethical ones.

Mechanisms for anonymous reporting must be trusted. If employees believe that reporting will lead to retaliation – even if it is not officially sanctioned – they will not report. Trust is built not through promises, but through consistent action. When reports are handled with confidentiality, when investigations are transparent, and when outcomes are communicated without blame, the culture begins to shift.

Without it, surveillance measures may breed resentment and increase retaliation risks. Monitoring without trust is not security – it is suspicion. And suspicion, when institutionalized, becomes self-fulfilling. Employees who feel constantly watched become disengaged. Disengaged employees become vulnerable. Vulnerable employees become risks.

In Serbia, where institutional trust remains fragile and bureaucratic culture is often hierarchical and opaque, the development of security culture is not merely an organizational challenge – it is a societal one. Training programs exist, but they are rarely evaluated. Reporting channels are available, but they are rarely publicized. Leadership speaks of compliance, but rarely of conscience. The result is a system that looks secure on paper but is brittle in practice.

Security culture is not something that can be mandated. It must be cultivated. And it begins with listening.

RESEARCH METHODOLOGY

This study uses a qualitative, multidisciplinary approach combining literature review, comparative legal analysis, and case studies from Serbia and international contexts. The data were drawn from academic sources, official reports (US Cybersecurity and Infrastructure Security Agency [CISA], International Business Machines Corporation [IBM], National Institute of Standards and Technology [NIST]), and documented incidents involving insider threats. The selection of sources was guided not by volume, but by relevance – by the depth of insight they provided into the human, organizational, and legal dimensions of insider behaviour.

Case studies – including Obradović, Perišić, and Milošević – were analysed to identify patterns in motivation, legal treatment, and organizational response. Each case was examined not in isolation, but in relation to the broader institutional context in which it occurred. What were the conditions that preceded the disclosure? How did the organization react? Was there any internal mechanism for addressing the concerns raised? Were the individuals involved given an opportunity to explain their actions? Were their motives considered, or were they reduced to a legal category?

Legal frameworks in the United States, European Union, and Serbia were compared to assess effectiveness and interoperability. The US model, shaped by Executive Order 13587 and NIST SP 800-53, emphasises centralized oversight and mandatory reporting. The EU's NIS2 Directive takes a risk-based, sectoral approach, integrating insider threat management into broader cybersecurity obligations. Serbia's framework, by contrast, is fragmented – a collection of laws that address aspects of the problem but lack coherence.

Machine learning and behavioural analytics were referenced where relevant to illustrate detection capabilities, but the focus remains on human and organizational factors. While algorithms can identify anomalies in data access patterns, they cannot interpret motive. They cannot discern whether an employee who downloads files at night is stealing for profit, or preserving evidence of corruption. They cannot understand the context of a workplace where reporting a problem has previously led to demotion.

The methodology emphasises ethical considerations, ensuring that discussions of surveillance are balanced with respect for privacy and whistleblower rights. This is not a call for less security – it is a call for smarter, more humane security. Surveillance without ethical grounding is not protection – it is control. And control, when applied indiscriminately, undermines the very values it seeks to defend.

The goal of this study is not to provide a universal solution. It is to illuminate the conditions under which insider threats emerge – and the conditions under which they can be prevented.

ANALYSIS AND DISCUSSION

Insider threats manifest in various forms: data theft, sabotage, espionage, and workplace violence. Psychological triggers such as perceived injustice or lack of recognition often precede intentional acts (Ruohonen & Saddiqa 2024) These triggers are rarely isolated. They are the culmination of repeated experiences – of being ignored, of being dismissed, of being told that your concerns are not important. When an employee feels that their ethical concerns are met with indifference, or that their professional contributions are undervalued, the sense of alienation grows. Over time, this alienation can transform into resentment. And resentment, when combined with access and opportunity, can lead to action – not always violent, but often disruptive.

Toxic work environments – marked by poor communication, discrimination, or fear of retaliation – exacerbate these risks (Center for Development of Security Excellence, 2024). In such environments, trust evaporates. Employees stop believing that the organization has their best interests at heart. They stop believing that leadership is competent. They stop believing that the system is fair. And when those beliefs disappear, so too does compliance.

Studies show that employees who feel unprotected are more likely to engage in retaliatory behaviour, including data leaks or sabotage (Center for Personal Protection and Safety, 2024). This is not irrational. It is rational within the logic of a broken system. If the organization does not protect you, you may feel compelled to protect yourself – even if it means violating rules.

Whistleblowers, though legally distinct, operate within the same access framework as insiders. Their actions, while potentially disruptive, serve democratic accountability. They expose waste, corruption, and abuse – often at great personal cost. Yet without adequate legal safeguards, they may resort to public disclosure out of necessity. In Serbia, Goran Milošević exposed EUR 6.5 million in toll fraud, leading to 41 convictions, yet was initially dismissed – a reflection of weak institutional support (Radomirović, 2015). His case is not unique. It is emblematic. It reveals a pattern: the state benefits from the exposure of wrongdoing, but punishes the person who made it possible.

This pattern is not accidental. It is systemic. It sends a message: speak up, and you will be punished. Stay silent, and you will be safe. The consequence is not fewer leaks – it is more dangerous leaks. Those who speak out now do so not through channels, but through media. Not to oversight bodies, but to journalists. Not to protect institutions, but to shame them.

Effective mitigation requires more than technology. Digital monitoring and anomaly detection are useful but insufficient alone. They can flag unusual behaviour, but they cannot judge intent. They can track file transfers, but they cannot understand why they occurred.

A comprehensive strategy must include:

- Clear policies on acceptable use and reporting channels – policies that are not buried in manuals, but communicated clearly, reinforced regularly, and modelled by leadership;
- Psychological assessments and conflict resolution mechanisms – not as tools of surveillance, but as instruments of care, designed to identify stressors before they lead to crisis;
- Training on ethics and information handling – training that goes beyond "don't click links" to ask "why does this matter?";
- Leadership-driven initiatives to improve workplace climate – initiatives that prioritize fairness, transparency, and dignity over control and compliance.

Organizations that foster transparency report fewer insider incidents and higher employee loyalty (Gelman et al., 2024). This is not coincidence. It is causation. When employees believe they are treated with respect, they respond with loyalty. When they believe their voice matters, they choose to stay – and to speak up – rather than to leave – or to leak.

The most effective insider threat program is not the one with the most sophisticated software. It is the one where employees feel safe enough to say, "I think something is wrong."

LEGAL AND REGULATORY ASPECTS OF INSIDER THREAT PROTECTION

International standards provide foundational guidance for managing insider threats. ISO/IEC 27001 outlines access control and risk management, while ISO/IEC 27035 details incident response procedures (ISO, 2022, 2023). These standards are not prescriptions – they are frameworks. They do not dictate what to do, but how to think. They emphasise process, accountability, and continuous improvement.

In the US, NIST SP 800-53 and Executive Order 13587 mandate federal insider threat programs (NIST, 2024; The White House, 2011). These are not optional. They are institutionalized. They require agencies to appoint insider threat officers, conduct regular risk assessments, integrate HR and security functions, and establish clear reporting pathways. The result is not perfection – but predictability.

The EU's NIS2 Directive requires member states to implement robust cybersecurity practices, including insider risk management (Directive (EU) 2022/2555). It does not prescribe how, but insists that it must be done. It treats insider threats not as an IT issue, but as a governance issue.

In Serbia, the legal framework consists of several laws:

- Law on Whistleblower Protection (Zakon o zaštiti uzbunjivača, 2014): it establishes reporting mechanisms and anti-retaliation provisions. Yet implementation remains inconsistent. Many institutions lack trained personnel to receive reports. Many employees do not know the mechanisms exist.
- Law on Classified Information (Zakon o tajnosti podataka, 2009): it regulates access to state secrets. It defines classification levels, but provides no guidance on what constitutes a public interest exception.

- Law on Personal Data Protection (Zakon o zaštiti podataka o ličnosti, 2018): it aligns with the General Data Protection Regulation (Regulation (EU) 2016/679), securing personal data. It protects individuals from misuse of their data – but says nothing about insiders misusing institutional data.
- Law on Free Access to Information of Public Importance (Zakon o slobodnom pristupu informacijama od javnog značaja, 2004): it promotes transparency. It grants citizens the right to request documents — but does not protect those who provide them.
- Law on Prevention of Workplace Harassment (Zakon o sprečavanju zlostavljanja na radu, 2010): it addresses abusive environments. It is rarely enforced. It is rarely referenced in security contexts.

A significant legislative update occurred in October 2025 with the adoption of the new Law on Information Security (Zakon o informacionoj bezbednosti, 2025). This law replaces the previous Law on Information Security (Zakon o informacionoj bezbednosti, 2016–2019), which ceased to be in force as of the eighth day after publication – October 31, 2025. According to Article 57 of the new law, the repealed legislation remains partially applicable until December 31, 2025, specifically regarding the transitional implementation of the provisions of Articles 6a–11b, 30, and 31. However, this does not affect the continued validity of the Law on Classified Information, which remains fully in force and continues to regulate the classification, handling, and protection of secret information.

The new Law on Information Security introduces a modernized, integrated approach to cybersecurity, emphasizing risk-based management, continuous monitoring, and cross-sector coordination. It explicitly supports the establishment of insider threat programs in critical sectors, aligning national practice with international frameworks such as NIST and CPNI. It mandates the appointment of Information Security Officers. It requires risk assessments that include human factors. It calls for interagency cooperation.

Yet, despite these advancements, the Serbian legal system remains fragmented. No single law comprehensively defines or regulates "insider threats" across public and private institutions. Whistleblower protections, classified information rules, and data security policies operate in parallel but lack full interoperability.

An employee who reports corruption involving classified documents may be protected under the Law on Whistleblower Protection – but prosecuted under the Classified Information Law. There is no mechanism to resolve this contradiction. There is no legal pathway that acknowledges both the public interest and the need for confidentiality.

To address this, de lege ferenda recommendations should include:

- Developing national guidelines for insider threat management, modelled on NIST SP 800-53 or CPNI frameworks – not as copies, but as adaptations, tailored to Serbia's institutional reality;
- Establishing a centralized program for high-risk organizations – not as a surveillance body, but as a coordination and support unit, helping institutions implement policies, train staff, and respond ethically to disclosures;
- Harmonizing whistleblower protections with cybersecurity obligations – so that disclosures made in good faith through authorized channels are shielded from prosecution under secrecy laws;

- Mandating the development of security culture in organizational policy – so that security is not seen as a technical requirement, but as a shared value, embedded in leadership, training, and daily practice.

Such measures would clarify the boundary between legitimate disclosure and harmful insider activity, enhancing both accountability and resilience.

CONCLUSION

Insider threats pose a persistent and evolving risk to information security. Their complexity arises not only from technical vulnerabilities but from human, organizational, and legal factors. While tools like user behaviour analytics enhance detection, sustainable protection requires a holistic strategy.

This study confirms that inadequate employee safeguards and poor organizational culture increase insider risks. Whistleblowers, though often conflated with malicious insiders, play a crucial role in exposing corruption and must be legally distinguished. Their actions are not breaches – they are corrections. Their intent is not to harm – but to heal.

For Serbia, the path forward lies in unifying its fragmented legal framework. By adopting integrated national guidelines and strengthening security culture, the country can better balance institutional protection with individual rights. This is not a matter of policy alone – it is a matter of principle.

Future research should focus on refining detection algorithms, evaluating cultural interventions, and assessing the long-term impact of legal harmonization. But even more urgently, research must examine the lived experiences of those who have spoken out – and those who have stayed silent.

Practical application: organizations should implement multi-layered insider threat programs combining technical monitoring, ethical leadership, and clear legal standards. Government agencies must lead by example, establishing cross-sector protocols that protect both data and democracy.

Security is not the opposite of freedom. It is its foundation. And when institutions choose control over conscience, they do not become more secure – they become more fragile.

ACKNOWLEDGEMENTS

The author declares no conflict of interest.

REFERENCES

Alsowail, R. A., & Al-Shehari, T. (2021). A multi-tiered framework for insider threat prevention. *Electronics, 10*(9), 1005. 1–18. https://doi.org/10.3390/electronics10091005

Center for Development of Security Excellence (CDSE). (2024, October). *Human resources & insider threat: Job aid.* Defense Counterintelligence and Security Agency. https://

www.cdse.edu/Portals/124/Documents/jobaids/insider/INT_Human-Resources-and-Insider-Threat.pdf

Center for Personal Protection and Safety (CPPS). (2024). *Understanding the relationship between insider threat and workplace violence*. https://www.cpps.com/insider-threat-and-workplace-violence/

Council of Europe. (2024). *European Convention on Human Rights: as amended by Protocols Nos. 11, 14 and 15 supplemented by Protocols Nos. 1, 4, 6, 7, 12, 13 and 16*. https://www.echr.coe.int/documents/d/echr/convention_ENG

Cybersecurity and Infrastructure Security Agency (CISA). (2024). *Insider threat mitigation guide*. U.S. Department of Homeland Security. https://www.cisa.gov

Delmas, C. (2015). The ethics of government whistleblowing. *Social Philosophy & Policy*, *32*(2), 79–103. https://doi.org/10.5840/soctheorpract20154114

Derikonjić, M. (2023, January 19). Perišić traži novo suđenje za špijunažu. *Politika*. https://www.politika.rs/sr/clanak/533341/perisic-vlajkovic-spijunaza

Directive (EU) 2022/2555. *On measures for a high common level of cybersecurity across the Union*. European Parliament and Council. https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

Gelman, H., Hastings, J. D., Kenley, D., & Loiacono, E. (2024). *Toward an insider threat education platform: A theoretical literature review*. arXiv (arXiv:2412.13446v1). Cornell University. https://arxiv.org/abs/2412.13446

Gheyas, I. A., & Abdallah, A. E. (2016). Detection and prediction of insider threats to cyber security: A systematic literature review and meta-analysis. *Big Data Analytics*, *1*(1), 1–29. https://doi.org/10.1186/s41044-016-0006-0

Greenwald, G. (2014). *No place to hide: Edward Snowden, the NSA, and the U.S. surveillance state*. Metropolitan Books.

Intelligence and National Security Alliance (INSA). (2022). *Strategies for addressing bias in insider threat programs*. INSA's Insider Threat Subcommittee. https://www.insaonline.org/docs/default-source/default-document-library/2022-white-papers/bias-and-insider-threat-programs-paper.pdf

International Organization for Standardization. (2018). *Information technology – Security techniques – Information security management systems – Overview and vocabulary* (ISO/IEC Standard No. 27000:2018). https://www.iso.org/standard/73906.html

International Organization for Standardization. (2022). *Information security management systems – Requirements* (ISO/IEC No. 27001:2022). https://www.iso.org/standard/27001

International Organization for Standardization. (2023). ISO/IEC 27035:2023 – *Information security incident management*. https://www.iso.org/standard/27035

Jeremić, V. (2024, July 31). Nova hapšenja u Krušiku, dok je slučaj Aleksandra Obradovića već pet godina u hibernaciji. *NIN*. https://www.nin.rs/drustvo/vesti/53680/uhapseni-radnici-krusika-pod-sumnjom-da-su-odavali-poverljive-podatke

National Institute of Standards and Technology (NIST). (2024). *Security and privacy controls for federal information systems and organizations* (NIST Special Publication 800-53, Rev. 5). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-53r5

National Protective Security Authority (NPSA). (2025) *Insider Risk Guidance.* https://www.npsa.gov.uk/specialised-guidance/insider-risk-guidance

Radomirović, V. (2015, May 8). Goran Milošević i Milovan Batak jesu uzbunjivači. *Cenzolovka*. https://www.cenzolovka.rs/drustvo/goran-milosevic-i-milovan-batak-jesu-uzbunjivaci/

Regulation (EU) 2016/679. *On the protection of natural persons with regard to the processing of personal data and on the free* movement *of such data (General Data Protection Regulation)*. European Parliament and Council. https://eur-lex.europa.eu/eli/reg/2016/679/oj

Ruohonen, J., & Saddiqa, M. (2024). *What do we know about the psychology of insider threats?* arXiv (Preprint arXiv:240705943 [cs.CR]. Cornell University. https://arxiv.org/abs/2407.05943

Schoenherr, J. R., Lilja-Lolax, K., & Gioe, D. (2022). Multiple approach paths to insider threat (MAP-IT): Intentional, ambivalent, and unintentional insider threats. *Counter-Insider Threat Research and Practice*, *1*(1), 17–34.

Singh, A. P., & Sharma, A. (2022). *A systematic literature review on insider threats*. arXiv (arXiv:2212.05347v1). Cornell University. https://arxiv.org/abs/2212.05347

The White House. (2011, October 07). Executive Order 13587: Structural reforms to improve the security of classified networks and the responsible sharing and safeguarding of classified information. *Federal Register*, 76(198), 63811–63815. https://www.federalregister.gov/documents/2011/10/13/2011-26729/executive-order-13587

Warner, M. (2014). *The rise and fall of intelligence: An international security history*. Georgetown University Press.

Zakon o informacionoj bezbednosti [Law on Information Security]. (2016–2019). *Službeni glasnik Republike Srbije*, 6/2016, 94/2017, 77/2019. https://pravno-informacioni-sistem.rs/eli/rep/sgrs/skupstina/zakon/2016/6/5/reg/20191108

Zakon o informacionoj bezbednosti [Law on Information Security]. (2025). *Službeni glasnik Republike Srbije*, 91/2025. https://www.paragraf.rs/propisi/zakon-o-informacionoj-bezbednosti-2025.html

Zakon o slobodnom pristupu informacijama od javnog značaja [Law on Free Access to Information of Public Importance]. (2004–2021). *Službeni glasnik Republike Srbije*, 120/2004, 54/2007, 104/2009, 36/2010, 105/2021. https://www.paragraf.rs/propisi/zakon_o_slobodnom_pristupu_informacijama_od_javnog_znacaja.html

Zakon o sprečavanju zlostavljanja na radu [Law on Prevention of Workplace Harassment]. (2010). *Službeni glasnik Republike Srbije*, 36/2010. https://www.paragraf.rs/propisi/zakon_o_sprecavanju_zlostavljanja_na_radu.html

Zakon o tajnosti podataka [Law on Classified Information]. (2009). *Službeni glasnik Republike Srbije*, 104/2009. https://www.paragraf.rs/propisi/zakon_o_tajnosti_podataka.html

Zakon o zaštiti podataka o ličnosti [Law on Personal Data Protection]. (2018). *Službeni glasnik Republike Srbije*, 87/2018. https://www.paragraf.rs/propisi/zakon_o_zastiti_podataka_o_licnosti.html

Zakon o zaštiti uzbunjivača [Law on Whistleblower Protection]. (2014). *Službeni glasnik Republike Srbije*, 128/2014. https://www.paragraf.rs/propisi/zakon_o_zastiti_uzbunjivaca.html