The Social Implications of NIST RMF

Kevin McFarland

Old Dominion University School of Cybersecurity

CYSE 525: Cyber Strategy and Policy

Professor Teresa Duvall

16 November 2024

The Social Implications of NIST RMF

The cybersecurity landscape has evolved in response to rapidly growing social and technological challenges, and the National Institute of Standards and Technology's (NIST) Risk Management Framework (RMF) was developed to address these emerging risks. The social factors driving this development include the proliferation of social engineering attacks, the need for stronger protection of private information, and the increasing digitalization of human interactions through social media. Despite the importance of these frameworks, evidence was not found where social media platforms have yet to adopt comprehensive security policies like NIST RMF, leaving users vulnerable to exploitation and manipulation.

NIST RMF Socially

The cybersecurity policy developed by the National Institute of Standards and Technology (NIST); The Risk Management Framework (RMF) had social factors that drove its development. These social factors may include social engineering, the need to protect private information, social science factors spelled out in criminological theory and the rapid digitalization of social relations via social media platforms. Ideally these social media platforms would also adopt NIST RMF as a method by which they would protect users' information, however no evidence was found of this. The personal information available and lack of cyber aware hygiene practiced on these social media platforms leave these users highly susceptible to social engineering. Grzegorz Strupczewski of the University of Economics Poland described the growing risk factors making NIST RMF implementation necessary, "The issue of cyber risk is continually gaining importance. It is evidenced by the increase in the number of scientific papers devoted to this topic. The concept of cyber risk is used in computer science, engineering,

business management, economics and social sciences (Strupczewski).” Social engineering has expanded to have an impact on all those mentioned areas.

The Internet has developed a rapidly growing structure in which economic and social relations are at risk of being a source of risky online behavior. This is one reason why organizations adopt NIST RMF, the security leaders of these organizations train their employees to help prevent these factors being an issue. Kevin Mitnick, a hacker-turned-security-expert, states in his book *The Art of Deception*, “Why are social engineering attacks so successful? It isn’t because people are stupid or lack common sense. But we, as human beings, are all vulnerable to being deceived because people can misplace their trust if manipulated in certain ways (Living Security Team).” It is this fallibility of users that organizations must stay ahead of, which makes NIST RMF use all the more necessary. In a conference held at NIST, given by S. Srinivasan a professor at Texas A&M University, he identified some social media security concerns, below is a selection: “

- Facebook users access the system mostly using cell phones
- This opens up free access to anyone getting hold of the cell phone of a user without the need for userid and password
- By default the privacy settings are set to Public, meaning anyone could see the profile and wall
- People have the habit of putting DoB, marital status, address, political beliefs, religion, hometown, etc in profile
- ‘Check-in’ feature in Facebook tells your friends your GPS location

- Login approvals can be created with code to other sites such as YouTube
- ‘Updates’ in Facebook are a dangerous way to let out too much information

(Srinivasan).” Its some of these simple details combined with some methods of social engineering that open the door for cyber threats to these organizations.

There is an additional concern which NIST addresses in separate publications, Artificial Intelligence (AI). In the Final Report from the Nation Security Commission on Artificial Intelligence, “The internet of things (IoT), cars, phones, homes, and social media platforms collect streams of data, which can then be fed into AI systems that can identify, target, and manipulate or coerce our citizens (Schmidt et al).” Which is the same thing that any hacker or cyber attacker might employ their skills to penetrate a system, just AI has the potential to do it much faster. The NIST AI RMF is combined with or even in addendum to NIST RMF, to help make a comprehensive system to protect data. With NIST eyes on AI, they seek help to assess and address risks associated with AI systems. There is considerable concern that AI poses a risk to national security, being used to target Federal Employees and systems by which, data can be extrapolated. For example, geospatial mapping combined with publicly posted fitness tracking data can reveal sensitive data about strategic infrastructure on U.S. military facilities. Another example according to a Special Competitive Studies Project (SCSP) adding national security concerns to NIST AI RMF, “Generative AI illustrates another novel risk of deep fake technology as evidenced by the U.S. Ambassador to Russia announcing that he was being impersonated by deep fake technology that was sufficiently convincing to fool some Ukrainian officials on video calls (Elluru et al).” It is aggregation of information that has become ubiquitous in the IoT world we live in that makes it so easy for cyber attackers to achieve their goals.

Conclusion

The development of the National Institute of Standards and Technology's Risk Management Framework is deeply influenced by the increasing social and technological challenges posed by the digital age. As social media platforms and other interconnected systems rapidly evolve, the risks associated with cyber threats, particularly those involving social engineering and the exploitation of personal data, have become more pronounced. Despite the growing need for robust cybersecurity measures there is a concerning gap in the adoption of comprehensive frameworks like the NIST RMF by social media companies, leaving user vulnerable to that exploitation and manipulation. The integration of AI technologies further compounds these risks, as AI systems have the potential to accelerate cyber-attacks, often exploiting publicly available data to target individuals and organizations. The vulnerabilities exposed by all this shows the necessity of adopting NIST RMF, which helps organizations address both current and emerging risks. Ultimately, as the digital landscape becomes increasingly complex, the continued emphasis on proactive risk management, cyber hygiene, and the responsible use of AI is crucial to safeguarding national security, personal privacy, and the integrity of our interconnected systems.

References

Elluru, Rama, et al. “National Security Addition to NIST AI RMF.” *Special Competitive Studies Project*, SCSP, Apr. 2023, www.scsp.ai/wp-content/uploads/2023/04/National-Security-Addition-to-NIST-AI-RFM.docx-1.pdf.

Joint Task Force. (2018, December). Risk management framework for information systems and... National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf. Accessed September 14, 2024.

Schmidt, Eric, et al. Final Report - Cybercemetery, NSCAI National Security Commission on Artificial Intelligence, https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf. Accessed 15 Nov. 2024.

Srinivasan, S. “Social Media Security: Protecting Privacy.” NIST Computer Security Resource Center, NIST, 27 Mar. 2012, csrc.nist.gov/CSRC/media/Presentations/Social-Media-Security-Protecting-Privacy/images-media/fissea-conference-2012_srinivasan.pdf. Accessed 15 Nov. 2024.

Strupczewski, Grzegorz. Defining cyber risk, Safety Science, Volume 135, 2021, 105143, ISSN 0925-7535, https://doi.org/10.1016/j.ssci.2020.105143. Accessed 15 November 2024

Team, Living Security. “The Evolution of Cyber Risk Management.” Living Security, Living Security, 21 Jan. 2023, www.livingsecurity.com/blog/cyber-risk-management. Accessed 15 Nov. 2024.