NASA Case Study: Cybersecurity Management and Oversight at the Jet Propulsion Laboratory

Minjoo Kim
Georgia Institute of Technology
Atlanta, GA, USA
Email: mkim908@gatech.edu

Do you think NASA would have written the same report if NASA had been responsible for the maintenance of the system?

In the decade leading up to 2019, NASA had several critical cybersecurity incidents that compromised major segments of its network. In 2011, for example, unauthorized entities gained full access to JPL's servers and stole 80+ gigabytes of data. Another example is the data breach that occurred in 2018, where an external user account was used to steal about 500 MB of data. Due to such threats to NASA's major mission systems, the Office of Inspector General (OIG) Office of Audits was led to write a comprehensive report that sought to provide an objective oversight of NASA's cybersecurity vulnerabilities.

OIG reports are usually quite direct regarding governance failures and are more willing to debunk technical shortcomings as much as possible. NASA could not do the same for several reasons. First, it is difficult for an entity to provide an objective evaluation about itself. If NASA wrote the report, it would have most likely downplayed its organizational accountability. It is also possible that NASA could have employed softer language to make the problems appear less serious. Also, most organizations justify their course of action to emphasize constraints. For example, there are often circumstances where an organization could ignore security flaws to escalate operational efficiency. In fact, the report clearly indicates that there were security problems with log tickets that were ignored for months.

How do you think JPL should resolve the issues in the report?

In the same report, there are several recommendations that OIG makes to mitigate future risks to the problems presented. The following list is the guideline specifically stated in the report to address the problems presented (NASA OIG, 2019):

1. Require system administrators to review/update the ITSDB
2. Segregate shared environments connected to the network gateway and monitor partners accessing the JPL network
3. Review and update ISAs for all partners connected to the gateway
4. Require JPL to identify and remediate weaknesses in the security problem log ticket process and provide periodic aging reports
5. Require validation, update, and performance annual reviews of all open waivers

6. Clarify the division of open responsibility for conducting routine log reviews and monitor compliance on a more frequent basis
7. Implement the planned role-based training program
8. Establish a formal, documented threat-hunting process
9. Develop/implement a strategy for institutional IT knowledge and incident management

Most of the recommendations are within the industry standard for maintaining a well-defined cybersecurity defense. It is crucial that JPL implement the guidelines into practice so that they prevent future attacks from happening further.

Why should policy match practice?

Policy should match practice because a good policy does not translate to value when it is not practiced. In the case of JPL, it is mentioned that the lab did have security protocols in place, but its inability to implement them into practice allowed cybersecurity attacks that compromised major segments of their systems. For instance, it is noted that NASA and California Institute of Technology signed a contract that required JPL to report certain cybersecurity incidents; however, there were no controls in place that ensured compliance with such requirement.

Reference

NASA Office of Inspector General (OIG), Office of Audits. *Cybersecurity Management and Oversight at the Jet Propulsion Laboratory* (Report No. IG-19-022). June 18, 2019.