Case Study: NASA

Georgia Tech

Case Study: NASA

- **Oversight report**, not incident report
- Report was **produced by an outside auditor - NASA Office of the Inspector Gen**eral as a review of the security posture of **Jet Propulsion Laboratory or JPL.**
- **Not extremely common** right now, but it could become more common as more people care about the **security of their data in the hands of a contractor,**
- It is also important to note that the Jet Propulsion Laboratory is **managed by Caltech, not NASA.**

Georgia Tech

Major Findings

Georgia Tech

- Failings are **catastrophic to their security** and the known cause of multiple incidents
- **Common** across both public and confidential reports
- **Most businesses** struggle with these issues
- Policies or best practices **had been outlined but were not the practice** followed by IT
- Generally the business goal is to create policies, practices, or procedures that will be the **most secure as they are actually implemented**

Major Findings

- Inaccurate and incomplete inventory
- Inadequate segmentation
- Legacy systems and lack of patching
- Ineffective exception process
- Inadequate log review
- Inadequate systems administrator experience training
- Improper incident response process

Georgia Tech

“A complete and accurate inventory of all devices connected to a network is critical for an organization to effectively monitor, report, and respond to security incidents in its network.”

Inadequate and Incomplete Inventory

Georgia Tech

"However, JPL did not properly segregate individual partner environments to limit users only to those systems and applications for which they had approved access. By properly segmenting a network, an organization creates boundaries an attacker cannot cross by eliminating connections to other systems. As a result, the shared environment lacked appropriate security controls to prevent partners from accessing a variety of exploration and human space flight mission data.”

Inadequate Segmentation

Georgia Tech

“JPL did not effectively address a known software vulnerability, first identified in 2017, with a critical score of 10. This software flaw can be used by cyberattackers to remotely execute malicious code, encrypt data on a targeted system, and demand payments to unlock the data.”

Legacy Systems and Lack of Patching

Georgia Tech

“Unnecessary waivers, extended waivers, and outdated compensating security controls expose the JPL network to exploitation by cyberattacks. While we understand the need to issue security waivers for particular systems, allowing waivers to remain open for an indefinite basis without periodic revalidation leaves systems with unresolved vulnerabilities and unapplied patches susceptible to attack.”

Ineffective Exception Process

Georgia Tech

“System administrators play an integral role in the overall security of IT systems within their control. Logs, which record events occurring on a particular system or network, provide valuable information for detecting and investigating malicious activity. Consequently, routine log analysis is a critical practice for identifying security incidents or policy violations and JPL policy requires system administrators to review system log files for suspicious or unusual activity on a regular basis.”

Inadequate Log Review

Georgia Tech

“Specifically, 9 out of 11 system administrators in our judgmental sample said they believed their routine analysis was no longer necessary once their system logs are sent to Splunk ES for collection and reporting.”

Inadequate Log Review

Georgia Tech

“According to training data we reviewed, all system administrators completed the annual mandatory cybersecurity training provided by JPL; however, this basic security awareness training alone does not meet NIST guidelines. Instead, NIST requires that organizations provide security-related technical training specifically tailored for their assigned duties.”

Inadequate Systems Administrator Training

Georgia Tech

"Specifically, the plan does not include, or only partially includes, the following elements:

- statement of management commitment
- performance measures
- mission statement (partially included)
- metrics for measuring the incident response capability and its effectiveness
- roadmap for maturing the incident response capability
- how the program fits into the overall organization
- annual review."

Improper Incident Response Process

Georgia Tech

How to Interpret This Report

Georgia Tech

The policy requires all systems be inventoried, but most aren't. **Why?**

Probably not malicious systems administrators

Not unawareness of policy

Probably not incompetent security team

A Thought Experiment

- Imagine every system delay costs **$100 in lost productivity**, 1000 systems delayed every year.
- **Annual cost of breaches is $50,000**
- The cost of following policy is **$100 x 1000 = $100,000**
- **$100,000 > $50,000** so the **policy is costing money**

Georgia Tech

Revisions to the policy that would have **allowed for risk acceptance**:

- They could have **removed the policy element entirely** and just stopped inventorying systems
- They could have **changed the policy to require that the inventory be reconciled on some schedule** and then implemented procedures to ensure this was followed

The problem: Management wanted security when it was an abstract concept but did not hold the line when the security policies required changes to business practices. They should have **decided to accept the risk or mitigate the risk in both policy and practice**.

What does this have to do with Incident Response?

- It's important to be aware that organizations are **very likely to fall for this trap** of making policies to mitigate risk generally but then **not making business decisions** to actually mitigate any risk
- It is likely that you will come across factors like these in your investigations and it is **useful to understand how a business gets to this point**
- It is important to realize the **disconnect between policy and management practice**

Georgia Tech