John Sikes
10/12/2020

**Legal Issues in System and Information Integrity**

In the set of the most recent revision of NIST's *Security and Privacy Controls for Information Systems and Organizations*, one control with a wide range of potential for legal issues is that of System and Information Integrity (SI-4). Despite the seemingly straightforward nature of monitoring a distributed system for unauthorized access and malicious actions, the true implications of the listed control are much more subject to legal difficulties. In particular, this family of controls doesn't effectively factor in the potential of rogue privileged users within a system's sensitive information range, as well as the results of anomalous incident analysis following successful detection.

With regards to the former of these issues, the family of controls for System and Information Integrity doesn't account for trusted agents acting against the controls and the group hiring such accordingly. While the set of controls does factor in limiting restricted user access and only providing specific capabilities to privileged users, it doesn't provide contextualization for an agent acting illegally of their own accord to, knowingly or not, sabotage and make unsafe an otherwise up-to-code operation. In doing so, while a company employing said agent may be following the family of control's word-for-word and maintaining a safe infrastructure, they may be undermined and rendered helpless if an agent under their wing actively works against them. This may be remedied, however, through other provisions within the context of the System and Information Integrity controls, specifically with regards to monitoring privileged users [SI-4(20)]. By following NIST controls regarding such, it would be possible to claim that detection was planned for such detrimental actions and the culprit was caught in the most expedient manner. However, this would not clear the company of legal issues in the case of multiple rogue users or of errors with monitoring said users accordingly. To this extent, legal issues abound within the confines of the realm of privileged users, and NIST has, presumably, done their best to provide controls and recommendations to handle such.

In a similar manner, the System and Information Integrity family of controls also doesn't effectively cover legal incidents in which an anomalous incident occurs, is identified early on, but is presumably resolved based on improper results drawn from its analysis. Given a situation in which this occurred, a company may believe that it has properly resolved the effective breach or otherwise malicious incident, however the resolution employed either handles a completely unrelated issue that may or may not have caused a similar incident in due time, or doesn't effectively patch-up the incident that caused the original issue in the first place. In doing so, the company in question could run into further legal trouble down the road, in which the same event occurs in identical or closely similar circumstances. Due to not properly resolving the incident the original time it occurred, the company would therefore not only be under fire for the incident occurring in general, but in further trouble of litigation as a result of allowing such an event to occur again, casting doubt upon the operation and safety of information in their possession. While this family of controls does provide ample requirements and recommendations regarding monitoring systems and their users [SI-4(4,24)],

it doesn't provide set requirements for resolution of incidents nor for unknowingly improper actions to resolve such. As a result, legal issues can be easily found and resolutions must be carefully implemented so as to maintain customer and regulator faith in one's operations.

The NIST family of controls pertaining to System and Information Security provides a significant amount of coverage regarding the regulation of system, information, user, and transaction monitoring. Despite all these controls and their enhancements therein, legal issues still arise as a result of unfortunate circumstances arising, with examples presented above with regards to malicious, trusted agents, as well as improper resolution of various incidents that may occur over a distributed system. In this manner, no means of control can guarantee complete protection from the unforeseeable, however the System and Information Security family of controls handles the vast majority of such cases and provides a skeleton for which companies can develop their culture to accommodate and resolve issues promptly.

## Works Cited

"Security and Privacy Controls for Information Systems and Organizations." 2020, https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.