John Sikes
11/5/2020

**Legal Issues in the Information Technology Sector**

In the domain of cybersecurity, very few fields are more paramount to protection and advanced detection as that of Critical Infrastructure. Pertaining to a variety of fields that are essentially to maintaining day to day life as we currently understand such, Critical Infrastructure can quite easily be understood to be a target of a variety of cyber attacks, along with simple setbacks in other fields causing severe issues in these. As with all incidents of normal functions being disrupted by accidents, oversight, or malicious influence, legal issues are abundant in Critical Infrastructure and, in particular, its Information Technology sector.

Defined by the Cybersecurity and Infrastructure Security Agency (CISA) to be “central to the nation's security, economy, and public health and safety”, the Information Technology sector of Critical Infrastructure pertains specifically to the processes by which hardware, software, and information technology systems and services are created, managed, and protected. As the world becomes increasingly connected by means of the Internet, it can be gleaned the importance of protection of these resources, both for general public safety (i.e. protection from identity theft) as well as that of government resources (i.e. data breaches revealing classified information). To this extent, CISA has defined a sector-specific plan that outlines the expectations of those working in and alongside the sector, as well as for the regulation of such expectations should one fall through. In this manner, legal issues crop up and industry members can find themselves in significant legal trouble as a result of their negligence or even pure bad luck.

For example, in the Sector Specific Plan for the Information Technology Sector, CISA denotes that a critical function of the sector, providing Internet routing, access, and connection services, has a serious risk of loss of routing capabilities through a manmade attack on the routing infrastructure. To mitigate such, CISA has stated that one of the mitigations currently being enhanced is that of responsiveness to increasing Internet traffic, with another being to increase physical security of access and exchange points. While these mitigations in the process of enhancement indicate a lack of cause of concern, the flip side is that both are wholly susceptible to manipulation on the side of the technicians in charge of such responsiveness and physical security, with negligence of duties and malicious activity on their part undermining whatever clever techniques are taken on the software side to prevent such. Similarly, another mitigation discussed by CISA is that of improving incident response by including contingency planning and training to properly monitor networks to identify and respond to outages or incidents. This mitigation has the same issues discussed with the former two, namely by being susceptible to the whims and negligence on part of the technicians working on the network, but also incurs further legal trouble if planned and distributed training doesn’t properly account for up to date issues and newly coming threats that are wholly unpredictable. Likewise, the discussion of contingency plans is also susceptible to lack of foresight by not properly accounting for catastrophes that could bring down a network necessary for

operation of a critical facility, which could even impact a hospital where a life can depend on such a network.

Due to the interconnection of the globe and all of technology through the Internet and embedded systems, CISA's plans and definitions for the Information Technology sector of Critical Infrastructure are increasingly more important than ever before. As a result of these plans and statutes, the sector is both better prepared for the expectations and standards by which it must abide, however legal issues can still arise when both the predictable and unpredictable strike. To this extent, risk must therefore be mitigated at all possible opportunities to properly avoid time in court, but also to save potential lives and maintain order where it's most important.

## Works Cited

"DHS Information Technology Strategic Plan 2019-2023." Department of Homeland Security, 4 Mar. 2019, www.dhs.gov/publication/dhs-information-technology-strategic-plan-2019-2023.

"Information Technology Sector." Cybersecurity and Infrastructure Security Agency CISA, www.cisa.gov/information-technology-sector.

"National Infrastructure Protection Plan." Cybersecurity and Infrastructure Security Agency CISA, www.cisa.gov/national-infrastructure-protection-plan.

"Security Tenets for Life Critical Embedded Systems." Cybersecurity and Infrastructure Security Agency CISA, www.cisa.gov/publication/security-tenets-lces.