

Your Fridge Knows What You Ate: Legal & Risk Management Solutions to Malware in the IoT

From coffee makers, to juicers, to refrigerants the number and type of devices connected to the internet of things (IoT) has been expanding rapidly. Frequently, these devices are insecure and designed to collect as much valuable consumer data as possible. With companies unwilling to protect consumers, jurists, politicians, and concerned consumers have begun to ask if there is a place for the law. This presentation says yes. First, this presentation discusses what the internet of things is and the malware which has proven to be a scourge in the IoT. Next, this presentation proposes three ways to help protect the internet of things: implementing a cybersecurity framework, creating an enterprise risk management (ERM) system, and establishing a compliance program. This presentation will provide an overview of all three solutions, giving practitioners the tools they need to start protecting their organizations. Cybersecurity is no longer just a question for an organization's IT staff. Professionals from across an organization need to be willing to protect the organization from cyberattacks. This presentation places a particular emphasis on the need for buy in from *all* members of an organization, especially key decision makers in the c-suite. Effective cybersecurity is *only* found when established protocols and procedures are followed and effectively governed. Finally, this presentation reminds attendees that there is no 100% effective "magic bullet" to solve all cyberthreats. Bad things will still sometimes happen to an organization doing everything right. However, effective ERM, compliance, and cybersecurity can reduce the likelihood of cybersecurity incidents, mitigate the harm caused by those incidents, and help prove to a court that an organization was not negligent.