Aligning Cybersecurity Incentives in the Internet of Things

The scale and scope of connected devices that make up the "internet of things" present a unique cybersecurity challenge, as one device's vulnerability can be a problem for the entire network. With incidents of ransomware, data breaches and distributed denial-of-service attacks on the rise, cyberspace is now an active warzone. The federal government is also a victim of this insecurity. Anne Hobson, a technology policy fellow at the R Street Institute, may have a solution to alleviate this problem.

In a recent paper, "Aligning Cybersecurity Incentives in the Internet of Things,"[1] Hobson proposes that, as a high-profile cyber target and large user of internet-enabled devices, the federal government should require its contractors be held financially responsible where their cybersecurity vulnerabilities create costs or liabilities for taxpayers. The new directive could be set by Congress, the White House or agency rule and would be verified during the federal acquisitions process. The paper proposes that federal internet-of-things vendors and contractors should purchase cyber insurance to transfer the financial and operational risks of cyber-attacks. As Hobson writes:

> In the case of a cyber-attack or data breach that stems from the insecurity of a contractor or vendor's system, the contracting agency…could have to expend resources on a host of ancillary costs, which can include DDoS mitigation services, forensic investigations, user notifications and data recovery. Rather than pass such costs onto the taxpayers, agencies and government purchasing agents should assert in contractual language their right to subrogate these liabilities from the contractor or vendor.

This would create a market-based incentive to adopt basic cybersecurity measures and improve the entire ecosystem. It would save taxpayer dollars by helping companies recover and by preventing high vendor turnover due to a cyberattack. Moreover, it will encourage cyber-insurance takeup more broadly, helping to increase the availability and affordability of cyber-insurance products. Lastly, it allows the government to set an example as a market participant by signaling to industry that it is serious about encouraging cyber-insurance adoption to bolster the nation's cyber preparedness.

---

[1] http://www.rstreet.org/thecyber