FTC Sends Warning to IoT Companies on the Importance of Secure Software Development with Enforcement Action Against D-Link

Internet of Things ("IoT") companies are on notice: the FTC is concerned about the the security of software installed to IoT and smart home products and is prepared to take enforcement action against companies to ensure that consumers are protected.

The FTC has just announced the proposed settlement of its case against D-Link filed in January, 2017, which mandates that D-Link put in place and maintain a comprehensive software security program for the next 20 years that incorporates certain specified requirements, including a "secure software development process" that incorporates specified software development safeguards to ensure the security of its devices.

These FTC imposed requirements include the following:

- Specifying in writing how functionality and features secure the devices;
- Engaging in threat modeling to identify potential security risks;
- Reviewing every planned release of code with automated static analysis tools;
- Performing pre-release vulnerability testing on each planned release of code;
- Performing ongoing code maintenance to address vulnerabilities as they are identified;
- Adopting remediation processes to address identified

security flaws at any stage of the development process;
- Monitoring research on possible vulnerabilities to devices;
- Setting up a process for receiving and validating vulnerability reports from security researchers;
- Making automatic firmware updates to devices;
- Notifying customers at least 60 days in advance of any decision to stop making security updates to a devices; and
- Providing biennial security training for personnel and any vendors involved with the device software.

In addition to imposing the above requirements on D-LInk, the order gives the FTC the power of oversight to ensure ongoing compliance, and requires D-Link to obtain routine third party assessments by a professional with credentials specified by the FTC to perform in-depth reviews of D-Link's security practices. The FTC specifically mandates that the assessment meet an approved standard as defined by the FTC: the International Electrotechnical Commission ("IEC") standard for the secure product development life cycle. The FTC announcement is attached **here** and its order is **attached here.**

What prompted the FTC case against D-Link? The FTC complaint filed against D-Link alleged a failure by D-Link to take "reasonable" steps to secure software constituting "unfair acts or practices in or affecting commerce, in violation of Section 5 of the FTC Act, 15 U.S.C. Sections 45(a) and 45 (n)" and misrepresentations regarding D-Link's security practices constituting a "defective act or practice, in or affecting commerce in violation of Section 5(a) of the FTC Act, 15 U.S. C. Section 45(a)." The FTC Complaint against D-Link is attached **here**.

What do companies engaged in IoT software development need to take away from this enforcement action? First of all, companies need to be aware that the FTC is applying its regulatory powers against companies to ensure that they are

securing software in accordance with any representations made to consumers. Second of all, companies need to be aware that the FTC is looking to certain published standards by the IEC to provide the industry standards for software in this space, so IEC compliance certification may provide the measure of a company’s compliance with its security obligations. Third, the FTC has provided some suggested guidelines for companies to follow in the following publications: **Careful Connections: Building Security in the Internet of Things** and **Start With Security: Lessons Learned from FTC Cases.**