ARTICLES

# The Internet of Insecure Things is Changing Risk Profiles

By Aaron Turner, Vice President of National Cyber Risk Practice at Risk Strategies

**Apr 1, 2019**

We're rapidly entering the Internet of Things (IOT) era; more and more connected devices are coming online every day, from consumer appliances to medical devices to self-driving cars. This exponential growth brings with it greater vulnerability due to an ever expanding attack surface.

While we haven't yet seen far-reaching cyberattacks targeting IoT devices, we will in the not-too-distant future. Given the rapid pace of change and possibility, cyber risk insurance policies written a few years ago may not have adequate language to cover potential losses and damages that today's IoT vulnerabilities expose. Now is the time to start reassessing cyber risk profiles in an IoT world.

**IoT cyberattacks will target new customer segments**

What would an IoT attack look like in the real world? We might begin to see ransomware attacks that target private consumers instead of large commercial enterprises.

Think about how many networked devices exist in a typical American household. Nest thermostats, Ring doorbells, video game consoles, routers, printers, smart phones and smart appliances like refrigerators are all connected through the homeowner's WiFi network. Much like they've targeted businesses in the past, hackers could hold homeowners' networks hostage until they agree to pay a ransom in bitcoin.

This is especially plausible considering the pressures in the consumer electronics industry to be first-to-market. As with any emerging technology, first iterations are not as well designed or as well thought out as later versions. IoT devices also generally tend to be less secure than commercial devices.

Another weak spot for an IoT cyberattack is public infrastructure. For example, let's say that a utility company is targeted. Today's smart utility grids feature networked sensors, two-way communication and AI-powered analytics to enhance machine intelligence and improve efficiency, emissions, reliability, etc. A hacker could gain access to the grid by entering through any one of its countless smart sensors and knock out power to an entire region.

**New network exposure, new types of loss**

What if someone dies because they didn't have access to heat or someone's house burns down because they couldn't call emergency services during a power outage? Does the utility's cyber policy cover those type of death and property losses? Death, personal injury and property losses are generally excluded by cyber policies, because when these policies were written these types of attacks were not a realistic proposition.

Today's cyber policies typically focus on financial losses including expenses that businesses incur to investigate the attack, determine financial liability, and reimburse costs for claims brought by regulators or individuals whose information was compromised in addition to business interruption losses.

Technology analyst firm Forrester says ransomware attacks on smart cities will be a new trend in 2019 and recommends cities invest in cyber security defenses to mitigate their risk.

As cyberattacks on IoT networks expose more potential losses, insurance carriers will learn from experience and adjust their underwriting and policy language. Buyers of cyber policies will, in turn, need to work with brokers who understand the nuances of the changing coverage landscape, and can coordinate policies that respond to these new types of scenarios.

*Want to learn more?*

*Find me on LinkedIn, here.*

*Connect with the Risk Strategies Cyber Risk team at cyber@risk-strategies.com.*

*Email me directly at aturner@risk-strategies.com.*

---

TAGS:
Cyber Liability