BRANDPROTECT EXECUTIVE THREAT BRIEF

brandprotect™

February 2016 | Briefing 14

THE IoT (INTERNET OF THINGS) AND YOU

YOUR ATTACK SURFACE WILL BE BIG. VERY BIG.

From GM OnStar, to the Google Nest thermostat. From your FitBit Charge activity and health monitor to your Philips Hue home lighting controller. The marketplace has exploded with new kinds of devices and appliances that use constant online connection to deliver new value to consumers. These devices are all examples of a new technology plane, the Internet of Things (IoT). **IoT is an emerging environment of physical objects that sense or measure their physical environment, and communicate those measurements via the internet to other devices and applications for analysis and action**. IoT apps use this data to make predictions, suggest or initiate actions, or manage processes.

Active sensing, the heart of the IoT, has been around for a while – think airplane transponder – but today's IoT world, with its rich array of personal and home devices and applications really originated with the launch of the first iPhone in mid-2007.

HOW IoT MAPPING APPS PREDICT DRIVE TIMES

Drive time estimates and traffic flow visualizations are a great demonstration of the power of the IoT. Essentially every smartphone in every car is an IoT device, constantly reporting its position to Apple or Google, who crunch that data to estimate the time remaining in your journey, and create the familiar green, yellow, and red traffic flow displays. When your phone's mapping app suggests that you go through the park, instead of around it, it's because it knows something!

26 BILLION IoT DEVICES BY 2020

Analysts predict that within five years there will be between 26 billion and 100 billion connected devices deployed world-wide. **Considering that the earth's total population in 2020 will be about 7.7 billion, that's 8-10 IoT devices per person, or 20-50 IoT devices per household**. Perhaps you have a few of these already.

BY 2020, THERE WILL BE AN ESTIMATED 8-10 IoT DEVICES PER PERSON, OR 20-50 IoT DEVICES PER HOUSEHOLD.

The IoT is much more than sleek looking wearables and thermostats – at the macro level, the data generated by these devices will create new efficiencies and drive a deeper understanding of individual and societal processes. From environmental management and supply chain optimization, to safer cars and more effective health care, there will be fantastic opportunities for new kinds of data-driven understandings, and powerful new business opportunities. But there are complications…. Every IoT device represents a point of vulnerability for the person or household that deploys them. Don't wait for a sensational story to run in the national press, take care today to make sure your devices are secured, and safe.

Remember, any device that is connected to the internet can be hacked by outside parties. Web cams and baby monitors are sometimes being accessed by nefarious third parties. Viral videos of well-intentioned hackers demonstrating how they could exploit vulnerabilities in IoT-connected automobiles are easy to find. And while the consequences of having your Bluetooth enabled health/activity sensor hacked might not be so ominous (do you really care if others know your heart rate?), you might feel differently if the hacked device controlled your home security system, had knowledge of your home and work networks or your personal contact list, or was your cardiac pacemaker. **Ransomware might take on a whole new dimension in the future.**

MINIMIZE YOUR RISK BY REDUCING YOUR EXPOSURE

At the personal level, although the IoT opens many doors, it does create some individual or family security risks. Luckily, these risks are easily mitigated by taking some simple common sense actions.

LOCK DOWN YOUR DEVICES

Obviously, the first step is to make sure that your internet connected devices are secured. If it is possible to implement a password (webcams, baby monitors, security systems), implement it.

SECURE YOUR HOME NETWORK

If your home wireless network is unsecured, secure it today. Do you broadcast your SSID? Do you need to? It's easy not to.

IMPLEMENT STRONG PASSWORDS

It's actually laughable that you can read articles that still list the most popular passwords as things like "Password" and "123456". Is the password for your home router still "admin"? Consider a change.

BE EXTRA VIGILANT WITH YOUR PHONE

Many IoT devices, from wearables to home appliances, rely on your smartphone as the primary interface to the device. Cyber criminals may try to exploit these apps as a way to gain control of your device. Only download IoT management apps from official stores. Do not experiment with third-party or aftermarket applications.

ALL ROADS LEAD TO YOUR PHONE.

The prize the hacker or cybercriminal is after is your phone. Considering what it carries -- and what could happen if the wrong third party could access it or control it – your phone is probably the most valuable item in your possession. Your phone carries information that could be considered to be a digital copy of you and your life. The data on your phone is a valuable commodity, it includes your network of friends and colleagues, credentials for the key networks you use, access to financial institutions, health care and insurance data, and access to your personal and work email accounts. IoT attacks are really just another way that the bad guys can get to your phone. Do your best to keep it safe from harm.

brandprotect™

www.brandprotect.com
sales@brandprotect.com | 1.866.721.3725

For enterprises concerned about their business exposure to increasing online risk, BrandProtect™ provides a complete suite of world class Internet threat detection services to monitor the entire social Internet spectrum and mitigate business risk arising from fraudulent or unauthorized online activity. BrandProtect helps security, risk management, and marketing organizations at leading financial services institutions, large-scale retailers, insurance providers, telecoms, pharmaceuticals and more, protect their brand value and business bottom line.