Internet of Things

A threat to Life and Property

by James Franklin
HDI Global Specialty

It's when we start seeing the small grey boxes being attached to mobile masts, lamp posts and appearing overnight on our streets like mini-telephone exchanges that we will know 5G has become part of our own lives.

This is not an alien invasion, it's just the science of 5G waves only travelling a much shorter distance than the current third and fourth generation we've become used to. We are trading distance for volume. Once this core infrastructure is in place we can say goodbye to buffering delays when downloading podcasts and throw open our arms, houses and bodies to welcome the hyper--connected, sensor-driven, super-high speed, and always-on future digital life.

The Internet-of-Things, or perhaps just "things" as we will start to call them in the near future, is largely a result of incredible cost-savings now achieved in the manufacture of microchips for mobile phones. When it costs a few billion dollars to set up a new manufacturing plant (or "fabs" as they are known) the economics and profit-motives of the process don't allow for much variation in the finished product.

It is now just too cheap and too tempting to pick up a box of ready--made, fully functional internet-

-enabled processors and put them in a new piece of hardware. The size, scale, range and function of such embedded devices is only limited by our imagination.

This last point is not a quality shared by the IoT. They exist in a product cycle that values the lowest cost and quickest speed to market. They are a product of a logical world where the 1's and 0's faithfully follow the command line and the guiding mind of many programmer/developers unknown to us.

We have created a handful of technological monocultures that have embedded themselves in life and property. This is fertile ground to conduct malicious operations. Those seeking to undermine data integrity and authentication know the end--users have no way to gauge the true intent of uploads, downloads, safety controls and other output.

So how does this play-out in real life...?

Sometime around 10 years ago the US Vice-President, Dick Cheney, had the Wi-Fi removed from his pacemaker. This was well before the hit TV show 'Homeland' depicted a cyber-based disaster scenario along such lines. The capability to cause harm was already available and felt to be "credible" and "accurate" even then. This technology is now becoming commonplace.

Also around that time, a "wireless infusion pump" for insulin was shown to release fatal doses without alerting either the patient or medical staff. Subsequently, a best practice guide on this subject has appeared in the NIST: 1800-8 Special Publication.

More recently, the gift of sight became possible using retinal technology. As NIST have since observed, the prospect of unintentionally glancing into the range of malicious QR codes that deploy ransomware is not now beyond the realm of imagination.

These examples can be immediately catastrophic at a personal level. More broadly, we can expect these gadgets to multiply in their billions over a longer time-period. It is sensible to assume no meaningful asset inventory will ever be kept. If we knew where they were, could we even get to them?

When dialing home to Earth the Voyager space probes, launched back in 1977, have only one number – the NASA Deep Space Network. In 2018 a long-running breach was discovered in their Jet Propulsion Laboratory caused by a non-inventory computer. A substantial amount of valuable data was removed by one of the most simple processors available – known as a "Raspberry Pi" (it costs around $25 and is popular with children as well as space enthusiasts). These risks do not go away.

It remains unclear if these simple embedded devices should be contactable at all once installed, or perhaps they are best left to expire after a certain amount of time. The current situation for them to continue receiving instructions and yet remain 'immortal' seems a little unfair on the rest of us.

This is not a situation that can be fixed but it can be managed. The insurance industry has a long--standing ability to do this better than most. Improving public-private partnerships is one way to go. We have a lot to offer. We cannot do it on our own. ●

Author's Note: This opinion has been written with apologies, inspiration and thanks to the IoT guidance from NIST and NCSC, Dan Geer, Bruce Schneier, Jim Waldo, Eric Rosenbach, Richard Clarke & Rob Knake.

James Franklin leads the Cyber Underwriting for HDI Global Specialty in London. He holds a worldwide remit and has supported some of the largest cyber insurance programs in the world. As a keen advocate of the 'maturity model' approach and engaging with innovative technology offerings James advises on adapting world-leading best practice to make it accessible outside the 'Fortune 1000'. James is an alumnus of Harvard Kennedy School where he focussed on cyber strategy, technology and public policy.