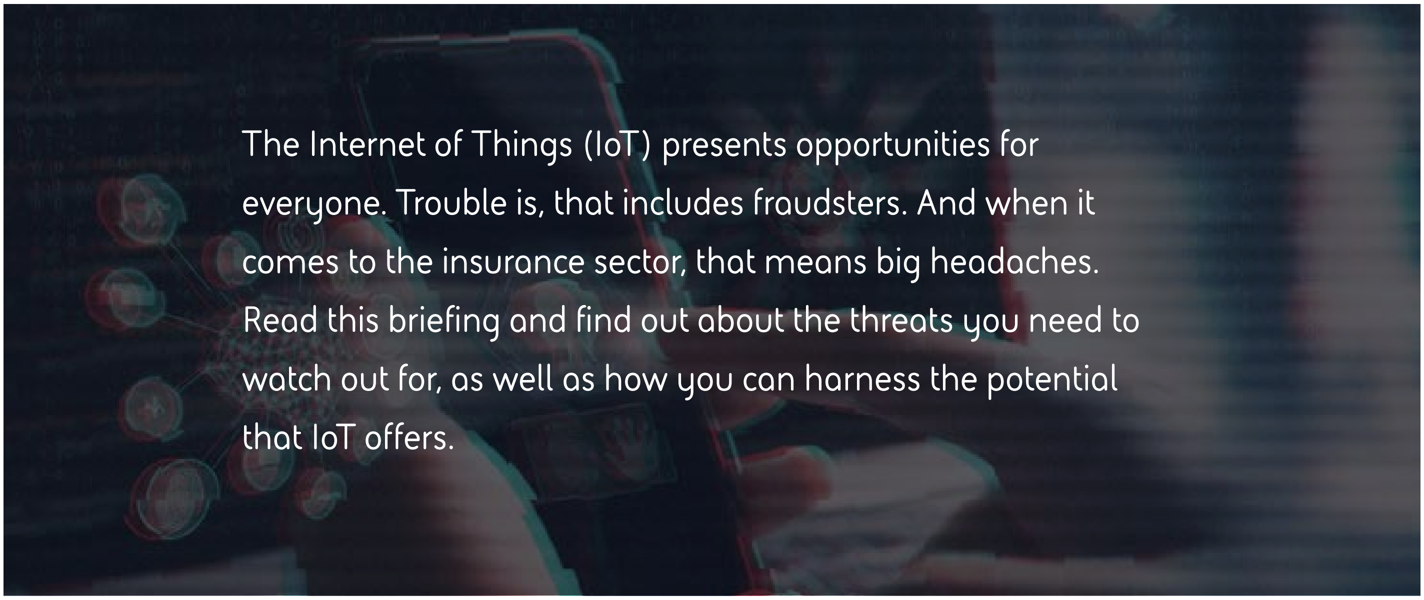
BAE SYSTEMS

Why IoT Could Make or Break the Insurance Industry

Insurance Insights

Tom Saminaden, Insurance Solutions Consultant, BAE Systems



The Internet of Things (IoT) presents opportunities for everyone. Trouble is, that includes fraudsters. And when it comes to the insurance sector, that means big headaches. Read this briefing and find out about the threats you need to watch out for, as well as how you can harness the potential that IoT offers.

Insurance in the IoT age

Pushing new boundaries means taking risks. And in the race to redefine possibilities for the Internet of Things, the very real risk is security isn't being prioritised.

Connected devices are making their way onto the market without the diligence and scrutiny many consumers take for granted.

Headlines are awash with warnings around IoT. A survey by Gemalto revealed most organisations (96%) and consumers (90%) are already demanding greater IoT security regulations[1]. But much of the media attention focuses on fanciful "headline hacks", rather than the more mundane (and more probable) vulnerabilities. Like fraud and identity theft.

And that's a big problem for the insurance industry.

The Internet of Things is a double-edged sword. For every opportunity, there's a sinister threat lurking in the shadows. Insurers can (and must) embrace the potential of IoT. But to do so they need to be fully prepared for this new era of hyper-connectivity.

That's where an intelligent approach to IoT comes in – helping you negate the threat of fraud and harness the full spectrum of opportunities.

[1] Gemalto, 2017: https://www.gemalto.com/press/pages/gemalto-survey-confirms-that-consumers-lack-confidence-in-iot-device-security-.aspx

What's the situation today?

Everyday items that surround us are getting smarter and more connected. From pens and toothbrushes to cars and shipping containers. And that means more and more data is being collected on our lives.

It's no surprise that the insurance sector has taken to IoT-generated data with gusto. The data generated from connected devices can provide valuable insight during the claims and loss adjustment process, giving insurers the opportunity to launch new usage-based products and speed up processing.

But questions remain around how (and how effectively) insurers are using this data. Specifically, despite this IoT data deluge, is sufficiently detailed information being collected to accurately determine a claim's validity?

Insurance evolution

Some insurers are already making strides in an effort to obtain a fuller data view – rewarding customers who supply them with IoT-fuelled information.

In the UK, Aviva is offering a motor insurance app that uses a phone's camera as a dashcam, providing a valuable record in the event of a claim. Aviva also discounts policies for motorists with an app score safer than average drivers. In the US, insurer Metromile offers policies payable by the mile thanks to its telematics system.

Other insurance markets also benefit from IoT. Neos offers reduced premiums for homes with connected smoke alarms and security systems – and offers customers such devices as part of its policies. US insurer Liberty Mutual will discount policies for customers who use Nest Protect-connected smoke sensors in their homes.

A natural naivety?

What all these innovations have in common is their innate "good persona bias" – where technologies or devices are designed assuming the user has virtuous intentions. And the predictable problem there? That's not always the case.

This rose-tinted perspective creates opportunities for fraudsters. Organised criminals are well aware of the potential security flaws that exist across internet-connected devices, and they are already familiar with the many ways they can be exploited.

And that's why IoT, as I've suggested above, is a double-edged sword. It promises huge potential for the insurance sector. But it's fraught with real risks, too.

So, just what are these pitfalls that await insurers?

The Threats posed by IoT

Hacking policy data

One of the immediate vulnerabilities that IoT can expose insurers to is the hacking and modification of usage data.

In an era when insurance is moving towards a pay as you go model, the ability to doctor policy or usage data is a concerning scenario. Such a situation would allow nefarious parties to affect premiums or trick providers with a faked low-risk profile. For example, the mileage recorded on a pay-per-mile policy could be manipulated and artificially lowered, or the time at which a vehicle is in use changed.

And if this sounds farfetched, it's troublingly feasible.

Just recently, the FBI warned that hackers were able to intercept ATMs and alter withdrawal limits[2] – potentially allowing limitless volumes of cash to be swiped. Fraudsters learn what works and replicate that model. And if it's possible to tamper with an ATM – a device deemed to be relatively secure – vulnerable IoT devices are an open goal.

Falsified claims

Fictitious or staged claims are an even more alarming concern; it has been reported that criminals are using peer-to-peer ridesharing companies to launder money through fake rides.[3] The fundamental flaws of IoT devices make it disconcertingly straightforward for fraudsters to fabricate collisions or damage and make a false claim. IoT opens the door to opportunistic criminals, and conceivably makes fraud easier, faster and more profitable than ever.

In the motor industry, intentional crashes are already a familiar fraud tactic. And despite its earnest intentions, IoT could conceivably reinforce fraudulent claims. By meddling with an Internet-of-Things-connected device, like a telematics box or a smartphone, fraudsters can stage fabricated collisions that are potentially harder to disprove.

And it's not just the motor industry that's affected. This approach could be adopted for fraudulent home insurance claims too. How can you verify if a smoke alarm was actually triggered? The same goes for a connected burglar alarm.

As IoT becomes more widely embraced, the challenge is finding a single version of the truth and being able to trust the data you're seeing.

[2] https://www.independent.co.uk/life-style/gadgets-and-tech/news/worldwide-atm-bank-hack-millions-stolen-withdrawn-warning-fbi-a8489931.html
[3] https://www.bbc.co.uk/news/technology-44355153

How to safely embrace IoT

Among all the murky forecasts, there’s good news though. IoT should be welcomed into the insurance fold. The sector just needs to be ready for it.

Insurers have access to larger data volumes today than ever before. But more information doesn’t necessarily mean better fraud prevention. Data needs to be processed in a timely and accurate manner to identify and thwart fraud. Smarter fraud detection platforms are therefore invaluable – capable of sorting through large volumes and varieties of data at speed.

Equally important is that data is sorted in a way that provides a single customer view; connecting the data collected by various devices to a customer’s profile provides better context around a claim and makes the job of assessing it – or identifying potential fraud – all the easier. Data consistency and alignment across all sources – quotes, policies, claims, credit data and device data – is vital when seeking out that single customer view. Just as important is seeing the connections between individual customers. Are two seemingly-unconnected claimants using the same email address, for example – or are there other, less obvious, connections?

It’s a big task, but one that must be diligently completed in the midst of a data deluge. And this is where the true power of a smart analytics platform can be felt.

Get prepared for the next gen fraud, now

There's never been a more exciting time for the insurance industry. But that breathless speed of innovation means risk as well as reward.

Find out more by visiting baesystems.com/**insuranceinsights**

Profile

Tom Saminaden,

Insurance Solutions Consultant, BAE Systems

Tom is a solutions consultant at BAE Systems, working across a number of insurance customer's. Tom has significant technical experience utilising Social Network Analytics (SNA) technology to detect both opportunistic and organised insurance fraud, at point of claim and policy inception, for some of the largest insurance companies and consortiums. Tom is fascinated by technology, probability and statistics and applying these to the financial crime problems our customers face.

BAE Systems, Surrey Research Park, Guildford, Surrey, GU2 7RQ, UK
E: learn@baesystems.com | W: baesystems.com/insuranceinsights
linkedin.com/company/baesystemsai
twitter.com/baesystems_ai