Pipeline
Technology for Service Providers.
www.pipelinepub.com Volume 15, Issue 4

What We Need to Do in the Fight against IoT Fraud and Identity Theft

By: Rui Paiva

Within just two years, it is expected that there will be four connected 'things' for every person on the planet. The growth of the Internet of Things (IoT) means more convenience and opportunity for more people, but it comes at a cost. With so many Internet-connected devices in every home and business, the IoT is a vast playground for fraudsters—and it's growing larger every day. Some 15.4 million consumers were victims of identity theft or fraud in 2017, according to Javelin Strategy & Research. In all, thieves stole $16 billion, making identity theft a very lucrative illegal business.

But many businesses are yet to heed the warning signs. According to a recent survey by Aruba, a HPE, 85 percent of businesses will implement an IoT strategy by 2019, driven by the need for innovation and business efficiency. But while businesses are forging ahead with their IoT visions, security and fraud management strategies have taken a backseat and businesses are leaving their front doors open for fraudsters to attack. In the same survey, 84 percent of respondents say they have already experienced an IoT-related security breach.

The financial gain for hackers looking to infiltrate the IoT lies in the data. In a rush to get items to market, companies often leave IoT devices unsecured and easy to access. Hackers can gain access to personal information that can then be used to create fake identities. Today, home Wi-Fi networks connect all our devices—and the valuable information within. A fraudster can hack into a Wi-Fi network through a connected refrigerator and be able to access your other devices, such as smartphones or a personal health tracker. A fitness watch or smartphone holds some of the most sensitive, unique data pertaining to you: your name, address, credit card information, photos, places you've visited, health information and more. From this information, along with social media, they can knit together a complete identity. Cyber thieves are extremely patient and will sometimes work for years creating files on their targets until they have enough data to start their scam. Maybe you post on social media where you went to college, or that your dad just retired from such-and-such company. Maybe your mom lists her maiden name on her Facebook account so her high school friends can find her. And most everyone posts the name of their dogs. Fraudsters know this information is often used to create passwords or serves as answers to verification questions.

Once personal information is stolen, fake identities have been created to buy expensive cars and purchase million-dollar homes, but sometimes the fraud is not as flashy—and is therefore easier to hide. In the U.S. a life insurance provider offered up to 15 percent off its policy premiums if customers wore a Fitbit to prove they were living a healthy lifestyle. In this instance, a fraudster could exploit your insecure device and steal health information and your records proving you ran five miles a day to get a much more favorable premium on their insurance policy. Automobile insurance providers are doing a similar thing with plug-in dongles that record driving metrics—and give discounts for those who don't speed or drive recklessly. A safe driver could have personal information stolen, which is then used by a bad driver who would otherwise be uninsurable or have to pay a heftier premium.

We have seen the results of security taking a backseat—and not only identities are at risk of being stolen. In another prominent risk, everyday appliances—such as lightbulbs, smart TVs and security cameras—have been hijacked and used to mount distributed denial of service (DDoS) attacks. In fact, DDoS attacks are typically just the first sign of bigger fraud problems to come, as fraudsters use DDoS as a smokescreen to slow down the response to the real issue, which is the fraud and theft that is actually taking place. It seems increasingly possible that a CCTV camera or a refrigerator can be commandeered into making calls to a premium number at $0.60 per minute instead of the local grocery store when you are next low on milk, allowing fraudsters to collect money on the other side.

This evolving landscape of fraud and identity theft begs the question: how do we protect our devices and our identities?

The Identity Theft Resource Center provides a number of recommendations to mitigate the risk of IoT devices being hacked. Its recommendations start by ensuring the IoT devices are only purchased by a reputable manufacturer with a track record of providing secure devices. Once IoT devices are connected, it is important to isolate them on their own protected networks, disable universal plug-and-play on routers and, if a device comes with a default password or an open WiFi connection, it is essential to change the password. Additionally, only allow the device’s operation on a home network with a secured Wi-Fi router. Remaining vigilant is key: always ensure that you update IoT devices when new security patches are released.

It’s also important to remember to attend to the security of an IoT device once it has been decommissioned. E-recycling initiatives provide important services that not only reduce electronic waste impact from physical devices but also ensure that they are thoroughly wiped clean of user information and any other data that you do not want exposed. It’s not just about identity data at risk of being stolen; a hacked IoT device can also provide a gateway to other associated devices and networks.

In the IoT world, finding ways to improve security to prevent these attacks is important, but security can only be the first line of protection, not the end in itself. After all, the end game for hackers and fraudsters doesn’t stop at just breaking into a web cam or another device—it’s the damage they do once they gain access that is the real problem. This reason is why security and fraud management must be tightly coupled together in order to address this risk.

Fraud management systems must work seamlessly with security protection to constantly monitor information across an organization, watch for unusual trends and identify fraud before it happens. That way, when security is breached, the fraud management system will be able to follow the breach’s path and identify patterns that reveal hidden relationships and suspicious movements and minimize any potential damage. In order to manage this, service providers must assess whether their current fraud management system is up to the IoT challenge. In particular, they need to ensure the core capabilities of their fraud management system include:

- Machine learning
- Self-service analytics
- Processing capabilities supported by Hadoop for continuous monitoring of huge data volumes
- Visual interfaces that help make sense of data in real-time
- Adaptive case management for and effective call to action
- Mobility

Underpinning these capabilities is the need for automation across the platform. When fraudsters access your network, the challenge is to single them out of the crowd, especially when they seek to trick your controls by replicating the behavior of ordinary customers. In addition, the interconnectedness of IoT means that an IoT attack cannot be contained to a single location. Simply put, the scale of IoT and the number of data points that traverse the network mean that service providers can no longer depend solely on human judgement. By implementing automated analysis, CSPs have the tools to combine data with context and to create the insights to make the right decisions at the right time. Automated analysis supports the most informed decision-making by repeatedly adding the latest data. And by providing an accumulated history, it broadens your perspective when assessing how to respond to suspicious behavior.

The IoT is a treasure trove for cybercriminals, offering up billions of vulnerable devices, a huge attack surface, no regulation and vast quantities of personal data. Cybercriminals and fraudsters are just waking up to what they can potentially gain from the IoT, and the market is being flooded with new ‘hackable’ devices every day. Businesses and homes need to prepare for this new world by having the tools and resources available to protect every bit of our identities.