3 location-based technologies reinventing data security

by ROMAN FOECKL — 16 days ago in INSIDER

Today's complicated data security landscape has begun to look a lot like a modern legend or fairytale.

Just like King Arthur gathered his knights to fight against enemies and supernatural forces to find the Holy Grail, organizations are constantly fighting hackers, malicious individuals and human error, seeking the "Holy Grail" of data security – making themselves virtually "un-hackable."

In security, there's a dangerous triad of motives formed by money, power and pride. This is because information is today's currency and the power one can get with the right information is priceless.

According to Security Intelligence, the average total cost of a data breach is continuing to rise by as much as 23 percent over the past two years to $3.79 million.

To address this, organizations need to create context-aware policies. This means that, to address increasingly sophisticated attacks,the security tools we apply need to take into

consideration more than anythingthe context in which data is being used.

Are employees accessing data on a smartphone? Do they have it stored on their personal laptop? Where does confidential data reside, and how is it being used? With whom is the data shared? How do you determine who is trustworthy?

We need to answer to all these questions to determine the context, and then come up with tools and policies that connect more to the reality of how organizations and employees are using data.

When creating security policies, most organizations currently take into consideration the job title and role of the staff. The manager usually has minimum restrictions, or none whatsoever. The accountant has access to financial information, HR to staff information, and so on. All of this is correct, but organizations also need to consider the circumstances employees are using the data.

Should the accountant have access to the company financial records when they are in the cafeteria? Is it enough to grant access to confidential information to the supervisor just because his job title implies he's trustworthy?

Enter the beacon

In the retail and advertising world, there has been a lot of talk about beacons (Apple calls them iBeacons™), which are small transmitters that constantly send a signal at a distance

ranging from a few inchesto a more than70 yards to all devices that are listening for such a signal.

If the device receives a signal and knows what to do with it, it will notify on the device screen with a message such as “here is something that might interest you,” such as a coupon or a special offer.

Total beacon shipments will surpass 400 million units by 2020, according to ABI Research and retail is only one market beacons have entered.

This incredible number is justified by the fact that the technology has applications in everything from enterprise, healthcare, smart homes, personal device tracking, IT security, and beyond.

Can iBeacons be used for InfoSec or other industries? You bet.

Before we speak about the role of beacons in IT security, I want to stress the importance and progress of indoor mapping and connect some dots.

Google vs Apple

In order to make use of beacons in data security, we need to consider the future of indoor mapping.

Google has come a long way with indoor mapping since launching the service in

September 2014 with six indoor maps. There are now indoor maps available in more than 20 countries, with thousands of floor plans.

Considering the short timeframe, this is amazing! We are also expecting rapid evolution, given the fact that venue owners can now upload their floor plans themselves.

Apple has the advantage of using iBeacons, which are designed to make Apple devices location-aware indoors. For example, if we are talking about a mall, aside from giving the exact location of a particular store, Apple can alsogive discount coupons. Information is adapted according to the venue.

Just imagine the possibilities for data security when it comes to iOS devices and Macs.

Now that every business owner can upload their offices' floor plan for both Android and iOS platforms, it is more convenient and important than ever to leverage beacon technology for information security.

Taking security to the edge with geofencing

Another way for organizations to make use of beacons is by combining them with geofencing capabilities.

With geofencing, companies can control access to devices, and applications on these devices, within a certain physical perimeter. It can be used both to keep information *in* by

restricting access to devices or applications such as the camera, AirDrop or iCoud while inside a company's perimeter, and *out* by making it impossible for devices outside the perimeter to access the network.

Real-world implementations

Banks or Wall Street firms use the Chinese wall to separate the flow of information to avoid conflicts of interest and leaks of corporate inside information. What if we can enforce this policy by adding even more context?

With geofencing technology, combined with beacons, these organizations can tell which part of a building an employee is in. Is there certain data that is not supposed to be accessed on the device while they have the possibility to meet people from other areas?

This system works because it doesn't just rely on the GPS location, but also uses local beacons to get a very precise idea of where the device is located.

Geofencing technology and beacons can offer an extra layer of security for enterprises trying to manage both company-owned and employee-owned devices. With a beacon placed at the door, or in a specific area of the office building, each employee can automatically receive Wi-Fi settings or have certain security restrictions based on the company's internal policy.

Healthcare is a another field with massive security implications. According to OCR, there were 253 healthcare breaches that affected groups of 500 individuals or more with a

combined loss of over 112 million records. Due to the high value and the fact that people's private information, healthcare records and bank information are all in one place, healthcare organizations have become a very attractive targets for malicious individuals.

Currently, mobile devices are used by doctors with minimum control from IT on what data they store or share. Sure, MDM solutions are enforced, but they are not always used at their full capacity.

With beacons, doctors can have patient charts automatically appear on an iPad when they enter a hospital room while the surrounding environment can be made more secure and compliant ensuring the patient's confidential data remains within the hospital.

Final thoughts and experimentation

Context-aware security solutions have caught a lot of attention, and the actions made by powerful companies show that they have a future across the board.

Beacons, indoor mapping and geofencing can and will be implemented in data security, not only retail, but across industries. We've already seen that location adds value and enriches the context for data security policies.

I'll leave you with an assignment that can lead to some interesting discoveries. Take the beacons, test them and let your imagination build new use cases and apply it to your own company infrastructure. See how you can improve security based on location.