IoT is listening, watching… | by Mike Smith AWS CCP
A tongue-in-cheek, but realistic scenario for IoT compromise

Your customers are complaining. And they make a valid point that your Internet banking application is unavailable inside your very own bank branch walls, because you don't offer free Wi-Fi in your 150-year-old stone building with no cell signal. Well shucks, that makes a lot of sense, doesn't it?

Now the employees are complaining that they can't listen to Pandora while churning out millions of dollars in mortgage documentation all day long. That seems fair, after all employee happiness and retention – especially a concern for younger generations – should be at the top of your list right below customer service.

So, the IT Committee advises, and the Board of Directors bites the bullet after so many complaints from customers and employees alike and decided to spend big money on wireless networking and security to support the new wireless initiative. After all, it is the Internet age; why not embrace it?

Your Information Security Officer and Infrastructure Manager are returning from lunch after celebrating the well-crafted, policy-driven, properly documented, properly segmented, and secured wireless network rollout for guest, employee, and corporate devices. A new age of employee efficiency and customer service has dawned within your institution.

As they skip down the hall in excitement, from the bank operations area they can hear *Money* by Pink Floyd booming out loud as the ops staff are grinding away at the new debit card rollout. That cliched song everyone in banking loves is emanating from an Amazon Echo right smack dab in the middle of the room.

The phone rings in the distance and someone says, "Alexa! Mute!" The music stops. Then another voice can be heard verifying customer identification, along with a repeated social security number, account numbers, balances, loan numbers and so on. Customers are served, made happy, and business is transacted. The call ends.

"Alexa! Unmute!" And the beat goes on.

The ISO drops to the floor having suffered a massive coronary and the Infrastructure Manager stumbles out the door and down the hall muttering something about dogs and cats living together, Faraday Cages, and switching careers. It's an unfortunate scene straight out of a Monty Python sketch…

Alexa has heard all about your customers' accounts, presumably ever since that Echo was purchased by the Operations Manager in response to a great month of deposits and the implementation of the wonderful new employee wireless Internet access benefit. And according to Amazon's responses to recent United States Senate inquiries, they keep that data forever, unless you deliberately and intentionally specify otherwise. But even then, Amazon makes exceptions.

You see, Amazon keeps "tracks" of voice data so that they can better serve their customers when making repeat inquiries or transactions. They justify this practice by saying the data is unindexed, or not searchable. They even "analyze" small portions to help Alexa recognize voice requests. That's right, their employees listen to you ordering your underwear off of Amazon. If you've already ordered a kind of pizza in the past, Alexa knows it. And she might influence you to order it again in the future.

As the United States Federal Trade Commission and the Department of Justice investigate business behavior in the markets served by Amazon, Google, Apple, and many other companies, it's up to you to protect your data. And it will likely remain that way forever, in spite of new laws and good intentions.

From regulatory and IT security points of view, IoT voice data collection security efforts and privacy efforts are akin to law enforcement in Dodge City in the late 1800s. As you digest that analogy, keep in mind it wasn't that long ago that

everyone had a tinfoil-hat reaction to the idea that your laptop camera was watching you, until it was discovered just how easy it is for a voyeur to eavesdrop on a compromised computer's camera, or to enable the microphone on a mobile device with the proper FISA warrant. Now we run around with tape or little plastic covers covering them (the first 5 people to respond to this blog receive a free 10-D camera cover).

Although not directly on the examiner's radar at the moment, technology like wireless or firewalls, an IoT policy that specifically outlines data security should be a priority for every Information Security Program. Consider developing one that includes steps to ban or secure devices, and to train staff on the proper application of mobile device and IoT security. You can bet this auditor will be asking about it during policy review.

Does your institution have an IoT security policy? Don't ask Alexa.