Compliance Today - August 2019
Ownership of healthcare data in the Internet of Things era, Part 3

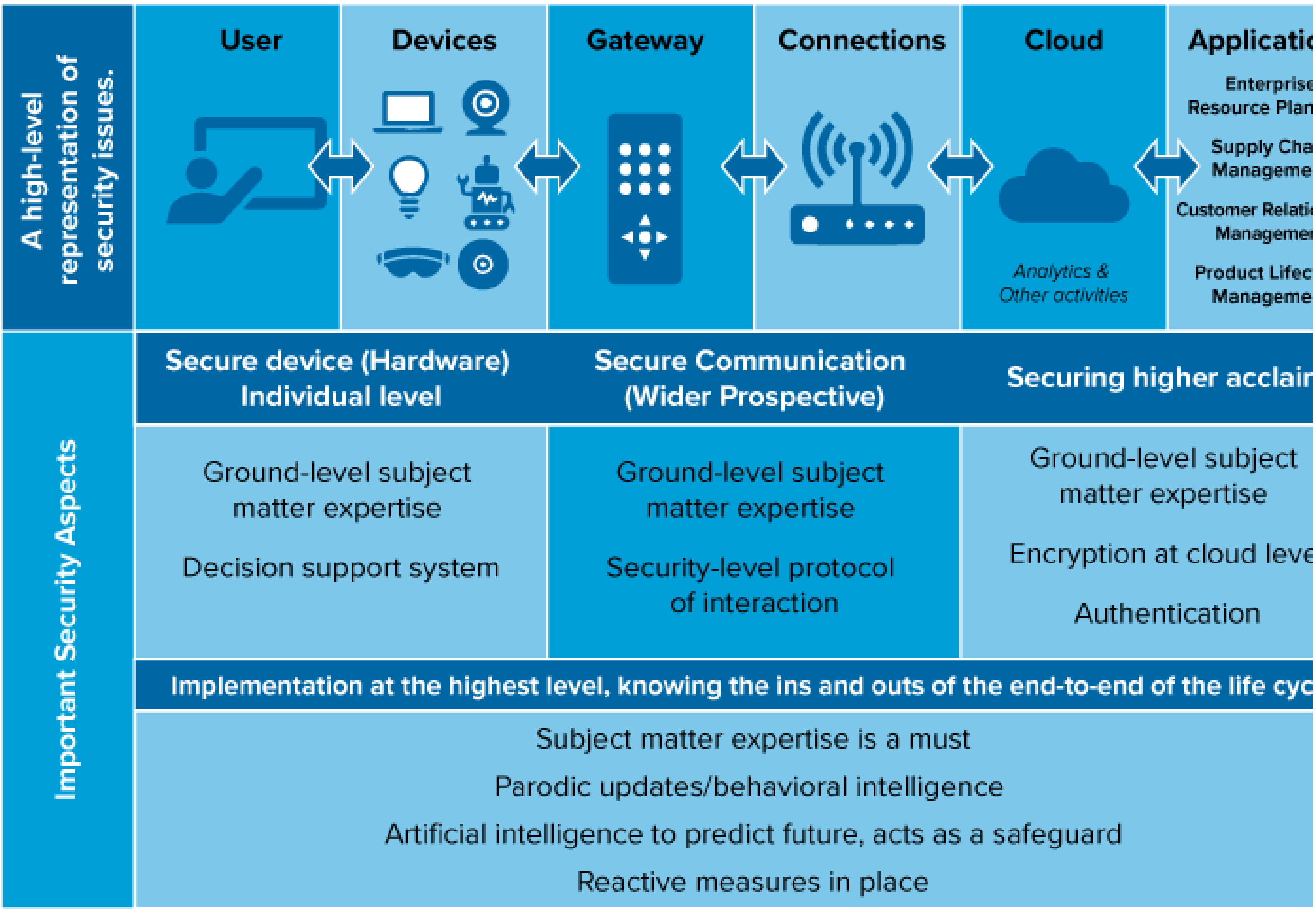
By Robin Singh, Ms(Law), MBA, Ms(IT), CCEP-I, CFE, HCCP

Robin Singh (robin@whitecollar.org) is Regulatory Compliance and Fraud Control Lead at an Abu Dhabi healthcare government entity in the United Arab Emirates.

This is the final part a three-part series which focuses on how the world of IOT works, its variabilities, and privacy concerns when it comes to a healthcare system. Part 1 was published in the June 2019 issue and Part 2 was published in the July issue of Compliance Today.

A total of 503 healthcare data breaches were reported in 2018, up from 477 in 2017, affecting more than 15 million patients. About 28% of these breaches were caused by insiders in some form or other, and about 44% were due to hacking, as reported by Protenus 2019 Breach Barometer report.[1] In the 2016 Protenus report, 27% of breaches were due to ransomware attacks. Again, this is just the beginning. It is estimated that nearly 20–30 billion devices in the healthcare Internet of Things (IOT) or Internet of Medical Things (IOMT) will be part of this growing ecosystem. For a high-level representation of security issues, see Figure 1.

Figure 1: Security issues with IoT devices



A high-level representation of security issues.

User

Devices

Gateway

Connections

Cloud

Applicatic

Enterprise Resource Plan

Supply Cha Manageme

Customer Relati Managemer

Product Lifec Manageme

Analytics & Other activities

Important Security Aspects

Secure device (Hardware) Individual level

Secure Communication (Wider Prospective)

Securing higher acclair

Ground-level subject matter expertise

Decision support system

Ground-level subject matter expertise

Security-level protocol of interaction

Ground-level subject matter expertise

Encryption at cloud leve

Authentication

Implementation at the highest level, knowing the ins and outs of the end-to-end of the life cyc

Subject matter expertise is a must

Parodic updates/behavioral intelligence

Artificial intelligence to predict future, acts as a safeguard

Reactive measures in place

Privacy aspect

Privacy in the digital age is a complex issue. However, here's the brutal truth: It is not even mildly realistic to think that privacy exists in the digital age. We have already, very willingly, divulged our private details to the online services that we patronize.

The problem with the IoT revolution is data privacy. A report called "Internet of Things: Privacy & Security in a Connected World," published by the Federal Trade Commission (FTC), found that around 10,000 households could produce over 100 million data points on a daily basis.[2] What that means is that hackers have over 100 million data points to exploit. To cut a long story short, hackers are going to have a field day.

Companies use collected data to assess an individual. For instance, your health data can be collected via a connected medical device and used by insurance firms to determine the kind of coverage you are eligible for. In fact, it's even possible for manufacturers or hackers to listen in on your conversations by hacking a device in your home or in your car.

For example, there is no law that prevents your internet service provider (ISP) from reading private emails and more importantly, that data can be obtained by law enforcement without even so much as a warrant.

According to the Electronic Frontier Foundation's Surveillance Self-Defense project site,[3] reasonable expectation of privacy ceases to exist the moment an individual gives up his/her information willingly. So, if you've uploaded personal details on Facebook, the social media platform has unrestricted access to it.

Closed-circuit TVs (CCTVs) have reaped an environment of caution and there is no doubt that with the use of IOT devices, the same can happen in the comfort of your home. In a car, a simple accelerometer and the gyroscope are capable of analyzing people's driving habits. Imagine what happens when the data available extends to the sleep patterns, smoking levels, and physical activity or movement/location and these can be used to derive information.

Data that was considered previously non-identifiable can become identifiable with the use of IOT devices, where people store most of their data. The reason for this is because the barrier between personal and non-personal identified information is greyed out. Patterns as simple as voice data and habit are good enough tools to identify individuals.