THREE QUESTIONS YOU NEED TO ASK ABOUT IoT SECURITY AND PRIVACY

Jessica Groopman, Analyst and IoT Advisor Newsflash ebook author

THREE QUESTIONS YOU NEED TO ASK ABOUT IoT SECURITY AND PRIVACY

Security in the Internet of Things calls for a completely different approach than that used for "traditional" Web-centric IT.

CONNECTING MORE THINGS CHANGES THE WAY WE SECURE THINGS

To understand the fullest context for protection requires organisations take holistic inventory, not just of their proprietary endpoints, devices and systems, but across all linked or associated devices, applications, networks, users and constituencies. Asking "what are we protecting?" is the starting point to: Identify this ecosystem Identify how the sensors and data we're adding to and collecting from products or infrastructure fit into that ecosystem This is a critical first step to developing a security strategy.

QUESTION 1: What are we trying to protect?

By its very nature, the Internet of Things is not one piece of technology, one business unit or one vertical. Rather, to deploy and connect devices, objects or infrastructure in an enterprise or consumer context inherently implies connections between multiple endpoints. Any connected application,whether a connected thermostat in your home or a fleet of sensor-clad wind turbines in the field, includes some configuration of devices, applications, networks and of course, people.

When taking inventory of the threat surface (i.e., the landscape of potential vulnerability), organisations must assess risks across the "IoT Security Stack. "These areas aren't just technological system components, but also the people and organisations who participate in the system, both internally and amongst partners.

THREE QUESTIONS YOU NEED TO ASK ABOUT IOT SECURITY AND PRIVACY

While device, application and network (i.e., technological) security are central to safeguarding any connected landscape, people represent another critical aspect of security that is often overlooked. Password security, BYOD environments, employee churn, lack of security training and simple human error are among the many risks that the human dynamic presents in any system. Remember, in the Internet of Things, a secure system is only as secure as its weakest endpoint. Empowering people helps strengthen security.

To understand the fullest context for protection requires organizations take holistic inventory, not just of their proprietary endpoints, devices and systems, but across all linked or associated devices, applications, networks, users and constituencies. Asking "what are we protecting?" is the starting point to:

*Identify this ecosystem
*Identify how the sensors and data we're adding to and collecting from products or infrastructure fit into that ecosystem

This is a critical first step to developing a security strategy.

Question 2: What would happen if our "smart" system was compromised?

In the event of an emergency, what happens? Many, many businesses today lack any idea — never mind a formalized and distributed plan — for what happens should they find themselves in a data, systems or physical security emergency, breach, hack or other compromise. Companies have a clear sense internally of:

THREE QUESTIONS YOU NEED TO ASK ABOUT IOT SECURITY AND PRIVACY

*What the threat surface is
*Where and with whom technology and systems components are associated
*What the actual threats are
*Where the threats may originate
*How to mitigate against those threats How to identify when an issue is occurring
*How to respond in the event a partner is compromised
*How to thwart, analyze, classify and communicate about the problem

They should also have a formalized plan in place for external communications about data-related crises — to partners, media and, most importantly, customers and end users.

As security practitioners plan for the what-ifs, they must recognize that IoT security requires a multifold approach that addresses legacy, current and emerging security challenges at once. First, organizations must meet traditional IT security challenges associated with legacy architecture and environments. Next, they must address the challenges introduced by our current generation of technology, characterized by cloud, social and mobile. Finally, as computing interactions and interfaces proliferate, as new classes of technologies emerge and as these interactions drive entirely new economies, organizations have an obligation to at least attempt to address the unforeseen, unintended and uncharted consequences of such digitization as best they can.

Question 3: What does personally identifiable information mean anyway?

Virtually every connected environment involves some element of personally identifiable information, also known as PII. If not data transmission, then data integration; if not integration, then employee or end-user associations. But thinking about security and privacy in IoT requires that we reconsider the very composition of personally identifiable information.

The definition of PII in the web 2.0 world enjoyed some clarification. The NIST Special Publication 800-122 defines PII as "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial and employment information."

As we transcend the laptop and digitize objects and environments, as we juxtapose, integrate and monetize diverse data sets from diverse environments, what is or may be "personally identifiable" is far less black and white.

THREE QUESTIONS YOU NEED TO ASK ABOUT IOT SECURITY AND PRIVACY

What is clear is that sensing technology is architected to sense physical realities: location, acceleration, temperature, heart rate, moisture, sound, light, position … the list goes on. And when these inputs are viewed in contextual spheres greater than themselves, they tell stories greater than themselves.

Fitbit's ability to track steps and heart rate generated the same data that revealed its users' sexual activity patterns, for example. The company quickly made such data — initially default set to public — private in response to outcry. Whether or not an individual's movement and activities through time and space are "linked or linkable" is unclear, both in the eyes of the law and in the eyes of those collecting the data. It's also unclear to end users generating the data:

*Are my comings and goings from my home personally identifiable?

*Is the way I drive my car personally identifiable?

*Are my biometric responses to stimuli personally identifiable?

Advertisers, insurance companies, manufacturers, retailers and employers are all vying to gain as much empirical context as possible, but where do we place technological limitations in favor of human sensibilities?

While no single organization can definitively answer these questions for every context, it is in its best interest to analyze the implications for use cases generating such data and how to manage and safeguard this data. In the event of a data breach, data malpractice or related crisis, such planning and documentation will help companies fare better in court. As businesses vie to collect as much data as possible, they must consider the unintended consequences of data collected and integrations with applications of such data.

THREE QUESTIONS YOU NEED TO ASK ABOUT IOT SECURITY AND PRIVACY

Questions reflect a new reality and demand a new IoT security approach

There are a variety of resources organizations can access to aid with each of these questions, but approaches to IoT security will vary. To aid in the quest to truly secure "Smart Systems," Harbor Research has developed a three-step process to guide organizations in their approach to IoT security.

While each of the above questions is central to an IoT security strategy, you might have guessed they are far from easily answerable checkboxes. Businesses must begin by assessing existing infrastructure, current development initiatives (including product, process and people), and align these against a larger enterprise strategy for both security and privacy protection. Forward-looking IoT security strategies begin with product design, but like IoT itself, they transcend products, across services, stakeholders, customer segments, threat vectors and lifecycles.

All IoT Agenda network contributors are responsible for the content and accuracy of their posts. Opinions are of the writers and do not necessarily convey the thoughts of IoT Agenda.