PADMASREE WARRIOR
Chief technology and strategy officer at Cisco

NETWORK SECURITY, REIMAGINED

by Derek Korte

AS TENS OF BILLIONS OF NEW DEVICES GET CONNECTED, BUSINESS AND SOCIETY MUST RETHINK SECURITY, PRIVACY, AND OPPORTUNITY

Illustration JUSTIN GABBARD

Smart networked devices are seemingly everywhere—as phones, bridges, jewelry, medical devices. Yet, by some estimates, only 1 percent of all potentially connectable devices are linked into a network. But they will be, very soon, and they'll change how we think about security and privacy. Padmasree Warrior is the chief technology and strategy officer at Cisco, and she believes that the emerging Internet of Everything offers both opportunity and pitfalls.

Cisco estimates that there could be 50 billion connected devices by 2020. How do businesses secure all of the new data generated by those devices?
Today's security models protect the endpoint, the data center, with firewalls and similar technologies. That model has to change to one that enables security across all of the devices and things that will be connected, from the browser to the boardroom. Security must also evolve from its current perimeter-based model. Companies used to buy a firewall and a content security solution, and then put the pieces together in the IT environment. We'll need to move beyond that to platforms that enable ambient security infrastructure and APIs to protect users and their data. We have to move away from point solutions to vendors that can provide end-to-end security solutions, or security as a platform.

What are the privacy implications of these changes?
Businesses must navigate the dilemma between privacy and personalization. The more information users give about themselves to the network and to the device, the more personalized that experience will be. This is the power of wearables and the Internet of Everything, but it intrudes on privacy. The only solution is to let users control the data.

How will they do that?
Today, opting in or opting out is a very rudimentary option. People don't know what they're opting in for or what they're opting out from. For example, when I log in to an app that asks me for permission to access location data, I usually say, "No." I don't know how I will benefit. Access to data must have more context to make it more useful and to guide users to make better choices. If the app said it wanted access to location data to guide someone to the nearest optometrist because the person's searching for glasses, then that's useful. Today, however, users often blindly opt in or blindly opt out.

How much of all this data will be personally identifiable?
That will be largely a personal decision. Consider a wearable that's microminiaturized and embedded in a user's body to collect information about health. It's personal information, but a user might want to share it with his doctor, as well. In business, we'll see data exchanges and value exchanges that will intermediate data so it can't be associated with a user or process. Data virtualization is already an emerging field, which virtualizes data without identifying the exact source.

THE ONLY SOLUTION IS TO LET USERS CONTROL THE DATA.

Are there special security implications in heavily regulated industries, such as health care or finance?
In the future, we'll need to focus less on securing the device or data, and instead strengthen security with policies around identification, verification, and authentication. However, the implications are more about privacy than security. People will want to ensure that information from their heart monitors, for example, is only shared with their consent.

What will technologists need to know to secure and understand the loads of new data generated by the Internet of Everything?
Every company must become a technology company. What's more, every company must also become a security company and understand the security implications in their business. That's a big shift. Also, IT and OT [operations technology] must come together. Take automobile manufacturers as an example. They typically have people who understand robotics, sensors, and automation and who build automated systems. That's called operations technology. They also have IT departments, which provide the connectivity and telecommunications solutions. In the Internet of Everything, these departments merge together. There will be more sensors on the manufacturing floor, so the people who design and build machines and automated systems must also understand the data that those systems and sensors create. In addition, DevOps has emerged as we move from a client-server model to a cloud model. In the old world, companies had developers and IT—and they didn't really get along. That's changing now as IT blends with OT under the cloud model.

Whose responsibility will it be to store, secure, and understand this data?
From an architectural point of view, the shift will require extending computer storage and networking to the edge, so to speak, where these devices and sensors connect. Part of that responsibility will fall to companies to deploy architectures and platforms that enable network storage. These can't be big systems. They must go out in a gas field or a manufacturing plant and be able to analyze data in real time. That will be the technology companies' responsibility.

The user's responsibility will be to make informed decisions about what he or she opts in for or opts out from. New companies will likely emerge that will help make those decisions more intuitive and more intelligent.

The challenges—and the opportunities—with the Internet of Everything will be dealing with data and turning it into action. That data must drive better business processes, which requires analysis. Businesses will also need to update their workforce's skill sets. We'll see new fields and new skill sets that will require an understanding of mechanical engineering, computer science, and data science.

What infrastructure changes will the shift to the Internet of Everything require?
From an infrastructure point of view, companies have to embrace two things: the cloud and connectivity platforms. There will be opportunities to create new kinds of applications, similar to when mobile became a platform. There will be a host of applications on IoE platforms that business will need to embrace, too. The Internet of Everything is not just about software or hardware; it's a coupling of the two.

Q&A with ANDREW ROSE,

PRINCIPAL ANALYST AT FORRESTER RESEARCH

The tens of billions of devices expected to be connected on the Internet of Everything within 10 years will represent a security challenge. Andrew Rose talks about the future of hacking in an increasingly connected world and what can be done to build security into devices from the start.

What are your most pressing security concerns?
The Internet of Everything is basically a massive data collection exercise. Once that data gets brought together, lots of what might be considered to be fairly trivial information can rapidly become very sensitive. Think about your food shopping. What you buy might suggest that you're a certain religion, and then that can be tied to your location, which shows that you go to a certain area on Sundays or religious holidays. Sensitive and private information can be derived from pretty trivial pieces of data when it's all gathered together.

But won't private information be anonymized?
There's going to be a lot of tension between marketing people who want to squeeze as much value out of the data as they can and the security guys who want to manage the privacy of data. And while we talk about anonymizing data, deanonymizing data that is not too difficult. A recent university study found that with just three pieces of key information – zip code, gender and date of birth – 85 percent of the information in a large database could be deanonymized.

What's being done to bolster security?
A lot of the time, the failure in risk management is just a failure of imagination. Security managers need to sit down and think through every possible scenario for this technology. And as these different platforms come together, we can't always predict how the result will look. Things are getting more and more complicated so if something goes wrong it's very difficult to troubleshoot and even more difficult to protect.

The Wright Brothers didn't delay the development of the airplane because they didn't have navigational guidance or oxygen masks. They just said, "Here's a plane, let's go!" That's how the Internet of Everything is coming together. The way forward seems to be manufacturers partnering with organizations that can provide security for them. We're seeing a number of security companies popping up now that actually provide a platform on which you can develop Internet of Things devices for the Internet of Everything. So you can still use all of your innovation and development techniques, but these security companies give you a way to communicate with other devices in a secure, encrypted way.