VANDERBILT

News

Who is Responsible for IoT Security?

By now, you've probably heard the conversation about the importance of the Internet of Things (IoT) security over and over again; the increased interconnectivity and communication between devices brings with it a greater risk for cyber threats and attacks. One small leak or breach on a single device can potentially spread across the cloud and create a noteworthy disruption within a company, affecting its assets, employees and customers.

But now that the risk factor has been identified and presumably understood, has it been made clear who is in fact responsible for carrying out IoT security? With many players involved in the operation and maintenance of security devices, uncertainty is understandable. According to a report from Radware, a provider of application delivery and cybersecurity solutions, there was no clear consensus among security executives when

asked who is responsible for IoT security. Thirty-five percent of respondents placed responsibility on the organization managing the network, 34 percent said the manufacturer and 21 percent chose the consumers using the devices as being primarily responsible.

These responses represent the truth of the matter: each one of these entities must take responsibility for contributing to comprehensive IoT security.

The Organization

It's not surprising that most respondents to the survey mentioned above chose the organization as the main stakeholder for IoT security responsibility; after all, if a company is managing a network, one would expect it to protect the network as well. This can be attained by adapting a user-centric design with scalability, tactical data storage and access with appropriate identification and security features (for example, the use of multilevel authentication through biometrics in access control). Organizations must also use their IT team to strengthen the overall cybersecurity of the IoT by keeping up with the latest software updates, following proper data-safety protocols and practicing vulnerability testing.

The Manufacturer

Manufacturers that provide IoT-enabled devices as part of a security system must be fully knowledgeable of the risks involved and effectively communicate them to the integrator or end user. Providing the education necessary and dedication to protecting users of its equipment makes a manufacturer more trustworthy and understanding in the eyes of an end user. Ensuring encryption between devices is a key step that manufacturers can take to work toward achieving complete protection in the IoT.

The User

Despite the protection delivered by the organization and manufacturer, there's always the option for IoT security to be enhanced or possibly even diminished by the individual user. It's critical that best practices for data protection are in place every time an individual uses a device that is connected to the network. These include disabling default credentials, proper password etiquette, safe sharing of sensitive information and the instinct to avoid any suspicious activity or requests.

The best way to clear up the general misunderstanding about IoT security responsibility is to emphasize that every contributor to the development and use of an IoT-enabled device plays an important role that cannot be dismissed. Despite the growing fear of threats to the IoT, the organization, manufacturer and user can work together and combine techniques to

form a guarded and secure system.

#ReadyForAnyChallenge