How Smart is Your Home?

by Sue C. Quimby, CPCU, AU, CIC, CPIW, DAE

THE INTERNET OF THINGS (IoT) is a term used to describe everyday objects that are connected to the Internet. Gone are the days when "high tech" meant a remote control for your tv or garage door. "Smart" technology offers convenience, energy, money and time saving, but it does have its drawbacks, particularly in the area of security. Helping clients understand and assess the pros and cons of "smart" technology is another value-added service of the professional insurance agent.

A smart home is one whose appliances, lighting, heating and or electronics can communicate with each other and be controlled remotely – either from another room or another part of the world. Systems can be run off a timer, or manually. Lights can be turned on and off, doors unlocked, or temperature controlled to name a few of the functions. This helps homeowners save money by using their appliances more efficiently. The global smart home market is estimated to reach $40 billion by 2020. 57% of users say that smart technology in their home saves 30 minutes per day. 47% of millennials already have some type of smart home device (https://www.alarms.org/smart-home-statistics/).

Security is the benefit most often stated as the reason for buying a smart home or smart home devices. Conversely, security concerns have deterred some consumers from purchasing smart technology. Hackers may be able to access systems, or the technology may fail. Devices such as Amazon's Alexa and Google's Echo are "always on". They start recording when they hear a "wake up" word. The technology is not perfect, however, and there have been cases where a device misinterpreted a conversation as the "wake" word and subsequently recorded and sent the conversation to someone on the owner's contact list. Hackers have accessed baby monitors to take pictures and post on the Internet, and threaten the family.

There are ways to make your smart home safer. Home routers and security cameras typically do not have any built in security. Give the router a name that does not attach to you or your home address, and use WPA2 encryption. Use strong Wi-Fi passwords, and do not share them. You can set up a guest network, one that is not connected to your smart home devices, for friends and family who need access. Be sure to update software. There have been a number of cases where a data breach occurred on a system when a patch to prevent the breach was already available. Two factor authentication is also recommended. If your system cannot be accessed without verification from your cellphone, it will reduce chances of hacking (https://us.norton.com/internetsecurity-iot-smart-home-security-core.html).

There are a myriad of smart devices sold by a multitude of vendors, accessed and controlled by a host of apps. Some are wired, where others operate wirelessly. Whether or not a hub is needed depends on the system involved. Smart hubs are a way to simplify and consolidate use of all of your home's smart systems. Some devices, such as Amazon Alexa, Apple Siri or Google Assistant, allow you to control your system with your voice. Some support multiple protocols. Others use apps on mobile devices. Some systems do not require a hub.

Advances in technology allow us to do things that were once the stuff of science fiction movies. However, with increased accessibility comes potential new hazards. Helping clients understand the benefits and drawbacks of being "smart" is another sign of the true insurance professional.

Previously published in the Insurance Advocate®