Connection Protection

Derrick Hughes
Vice President, Reinsurance, Assumed and Strategic Products, The Boiler Inspection and Insurance Company of Canada

The connected home, including smart appliances, is transforming everyone's lives. What are the challenges, risks and risk management strategies to address this transformation?

What is the connected home?

Consider that a homeowner is returning home in the middle of the winter after an exhausting day. The home's thermostat was automatically turned down in the morning to save energy, but upon arrival, it is toasty warm, the blinds are down, lights are on, music is playing, and the oven is preheated. Later in the evening, the dishwasher and washing machine automatically start to save on energy costs.

It is not science fiction — all of this has been automated through a smartphone, which remotely controls devices connected to home systems and appliances. The connected home can align every electronic piece of equipment through networks — computers, televisions, appliances, HVAC systems, door locks, thermostats, garage doors, motion sensors, cameras, water-leak sensors, light bulbs and switches, smoke and carbon monoxide detectors, plugs, outlets, power strips and music systems.

GROWING MARKET

By 2018, 46% of polled Canadian consumers will either own or say they plan to purchase connected home technologies, notes Nielsen's *Connected Home Report* from last November. One simply needs to step inside any retail electronics showroom to find more appliances hitting the market with connected capabilities.

And P&S Market Research reported just this past June that the global connected home market is expected to grow at around 14% in the next five years, owing to advances in electronics and communication technologies. Geographically, North America has been the largest market for smart homes, whereas the market is expected to witness the fastest growth in Asia-Pacific during the forecast period.

Higher purchasing power and changing lifestyles are driving the demand for smart home appliances worldwide, which include smart washers and dryers, air conditioners, smart water heaters, ovens and robotic vacuum cleaners.

Demographics, energy costs driving adoption

Experience to date suggests the under-40 age bracket will be the largest demographic driver of this market. Increasing purchase of connected home systems by high-net-worth homeowners for new home construction is also expected.

At the same time, traditional medical care is rap-

idly changing, driven by an aging population. That will likely result in the elderly wanting to remain in their homes for as long as possible, driving the demand for remote medical care that can be delivered in the home.

A variety of technologies — including motion and temperature sensors, cameras and wearable monitors — will enable caregivers to actively monitor the activities of aging occupants, to ensure they are safe, eating properly and taking their medications.

The desire to control energy consumption is another driving factor. Smart appliances and home systems interface with smart electrical meters to help manage energy use, lower costs and maximize efficiency. Homeowners are now able to optimize their bills by automatically shifting home electrical usage to periods when rates are the lowest.

Driven by these trends and the desire for voice-activated devices, vast financial investments are being made in the field, especially by very large companies with infrastructures and resources to quickly access the market and drive growth.

CYBER SECURITY A CONCERN

Most people do not think of home appliances as computers *per se*, when, in fact, the opposite is true: Manufacturers place hardware into appliances, enabling Internet connectivity within them to allow for remote control, automation and communication with other home appliances and devices. They are exposed to the same cyber concerns as are laptops, tablets and smartphones connected to the Web.

A 2017 report from Symantec notes a botnet, or a "zombie army" of connected devices infected with malicious software, can be controlled without owners' knowledge. An attacker can use the controlled devices to carry out malicious activities such as distributed denial of service (DDoS) attacks or spam campaigns.

Last October, home routers, digital video recorders and mostly Internet-connected cameras were reported to have enabled the biggest DDoS attack seen to date. DDoS attacks can affect businesses and consumers alike, and malware placed on a wireless router could conceivably lead to personal information being stolen, including user names, passwords and financial data.

Home devices an attractive target

Connected devices were primarily created for convenience, not security, and manufacturers are in the business of developing products at attractive prices to consumers. So, while more and more connected devices are becoming available, security is often not a priority for the manufacturer.

Most people do not think of home appliances as computers *per se*, when, in fact, the opposite is true.

This has led to poor practices such as the use of default passwords — for example, "admin" — which are often not changed by the end-consumer. These default passwords on devices give attackers easy entry into their owners' lives. Furthermore, devices often do not have built-in mechanisms to receive automatic firmware updates, resulting in vulnerabilities being left unpatched.

Manufacturers could be doing more

Many device manufacturers could be doing more to ensure security by making the issue a priority. Consumers think nothing of regularly updating software and apps on their computers, tablets and smartphones. Why would connected home devices be any different?

Since connected home devices have significant computing and connected capabilities, manufacturers should become more diligent in providing regular firmware updates.

Consumers also need education about security and manufacturers must include easy-to-understand directions on how they can keep their devices secure.

Security regulation required

In Canada, no single government agency oversees regulation of connected device security practices. The Office of the Privacy Commissioner of Canada is calling for regulation, stating the "technological development in the context of the Internet of Things has not been matched by an equivalent evolution of overarching privacy governance models. Not much consideration has been given as of yet to the many privacy implications of having an extraordinary amount of data points that could be collected, aggregated across devices and analyzed not only by the device owners, but also by other third parties unknown to the individual."

PROTECTING THE CONNECTED HOME

The first line of defence for protecting a connected home involves securing the router. It is generally advised to not use the router as configured out of the box. The following recommendations should be at the top of the security list.

Change router's default network name

Home routers/firewalls often set the default SSID (service set identifier) to something that describes the specific hardware (for example, Linksys). From a hacker's perspective, knowing the specific hardware platform that he or she is planning to attack makes the job easier. Use a random, innocuous name.

Change router's preset default password

Router passwords are well-known and well-documented. Change each administrative password to a strong complex password. When setting passwords, use upper and lowercase characters, include at least one "special" character and do not use any personally identifiable information in the name.

Disable guest access

Though allowing guests to access a home network may seem like a nice, convenient thing to do, users should be wary about allowing any "non-authenticated" users to access a homeowner's network.

Use WPA2 to encrypt network

The older WEP protocol has serious weaknesses and is easily compromised. While Wi-Fi Protected Access 2 (WPA2)

is not infallible, it does provide a higher level of security and is significantly more difficult to compromise. Once the Wi-Fi network is secured, look at each home automation device being installed. Securing specific devices will depend on their individual capabilities. At a minimum, the following is needed:

- *Generic email:* If the device has the capability to notify the user via email, set up a generic email account. Do not use a personal email account or server.
- *Mobile security:* Install mobile security software on the devices used to control the home automation devices (for example, smartphone). It is often easier to exploit a mobile application instead of hacking the device directly.
- *Patching and updating firmware:* Regularly check for firmware updates and install updates as soon as possible.
- *Disable Internet access:* If the home automation device does not need access to the Internet, disable its access within the firewall.

COVER FOR HOME CYBER RISKS

Cyber insurance, largely the domain of commercial lines, has recently crossed over into personal lines, with reinsurers offering endorsements for homeowner and tenant property policies. Such endorsements generally include coverages for computer attack, to recover data and restore systems; connected home device attack, to restore devices connected to the Internet; cyber extortion, with professional assistance on how to respond to a ransomware attack and payment of ransom when approved; data breach, including forensic IT and legal reviews, notification and recovery services when private non-business data entrusted to an individual is lost, stolen or published; and online fraud, for losses related to identifying theft, phishing schemes, illegal bank and credit card transfers, forgery, counterfeit currency and other deceptions.

As the insurance industry continues to address home cyber security concerns with coverages, services and education, homeowners will become more eager to adopt the technology to make their homes more comfortable, efficient and secure.

Editor's Picks

Looking for more information about connected homes? Check out www.canadianunderwriter.ca and search for the following:

- Home telematics startup Roost closes second round of funding with investments from Desjardins Insurance and Aviva Ventures
- Price continues to be hurdles to adoption of smart home devices: survey
- Smart home technology can be used to reduce potential claims from inclement weather, other risks: Allstate Canada