THE WIRE REPORT

THURSDAY, OCTOBER 17, 2019

News

Internet Society lobbies onproject to get ahead of IoT vulnerabilities

The Canadian chapter of the Internet Society (ISCC) is looking to embark on a broad scale project involving foreign and local governments, civil society and industry to tackle the security challenges of a quickly emerging technology: the internet of things (IoT).

The advocacy group has tasked its special advisor Jeremy Depow and its executive director Franca Palazzo to secure a funding commitment from the federal government to round up major stakeholders to propose standards for those connected devices.

The group filed a registration on Oct. 11 with the federal lobbyist registry to fund its "Mitigating Consumer Cybersecurity Threat Project." Its focus will be on educating Canadians about best practices to insulate them from threats and to identify standards, responsibilities and labelling of devices to ensure they are secure.

"What we're looking at is what minimum security standards an IoT device should have and what label will be attributed to that, and then how do we make sure consumers are aware of what they should be looking for when they purchase a device, so there are a lot of factors," Palazzo said in a phone interview.

"It's very important to have some sort of framework that is at least similar across the globe and so it's important to coordinate -- not necessarily to have the exact same regulations and frameworks in place -- but something similar," Palazzo said.

The project, which began being drawn-up about a year ago, is expected to be developed over the next year and will yield reports about the initiative's progress, Depow said, adding an advisory committee is currently being formed. Depow did not say how much money the organization is seeking from the government.

Palazzo added that the initiative is new, at least for the ISCC, in that it attempts to bring together international allies to the table -- versus previous versions that were more domestic in nature.

The federal government has recently completed one part of an IoT security multistakeholder project, which produced a framework that will be continued by the ISCC project, Palazzo said.

"We are usually behind when it comes to technology in terms of governance and safety; we're constantly playing catch-up. It's something that needs to be addressed," Palazzo added. "Connected devices offer huge benefits and opportunities, so we just want to ensure that we do all that we can to make sure that they are as safe as possible."

The number of global internet-connected devices is expected to exceed 25 billion by 2020, according to a national cyber security strategy document. They include "smart" devices like internet-connected refrigerators, toasters, dryers, baby monitors, cars, pacemakers and critical infrastructure. The wild west of IoT devices means some may come with completely insecure, with easily-decipherable passwords -- as was the case in one such cyber attack -- or no passwords at all and, in other cases, they could be used to hold information ransom or come equipped with spyware.

Bloomberg reported late last year that China was creating tiny chips and embedding them in the supply chains of giant U.S. companies.

"We are already seeing vulnerabilities and we're already seeing things happening," Depow said, when asked about why the organization decided now was the time. "There's not enough dialogue happening to make sure that we move...in the right direction."

There has, however, been sporadic dialogue at several conferences over the past couple of years. In 2017 a high profile cyber strike known as the WannaCry ransomware attack infected over 200,000 computers in at least 150 countries. That was a year after millions of insecure devices were used as conduits to launch a flood of traffic to domain name provider Dyn, which resulted in a number of websites being taken down internationally. Those kinds of attacks are still dogging Canadian business, according to the Canadian Internet Registration Authority.

Experts have been sounding the alarm about the dangers, imploring the government to get in touch with technologists and consider even adopting import standards for such devices. The United States Congress twice failed to pass similar bills in 2017 and 2018 that would impose standards for IoT devices purchased by the government, but the issue was reintroduced earlier this year.

Christian Tacit, a lawyer who has represented the Canadian Network Operators Consortium (CNOC), has raised the issue of a lack of regulatory certainty surrounding these devices on a number of occasions and challenged Innovation Minister Navdeep Bains to do something about it. At a conference in 2017 he wondered whether "we're not going to see a debate in the coming months and year or two about setting technical standards for IoT devices."

Innovation Canada is just one of several departments, including Public Safety, that the ISCC expects to reach out to, Depow said.

And still, at another conference, privacy and security experts in 2017 said the advent of the hyper-connected 5G world will bring about security and privacy risks, including with IoT devices. A Blackberry Ltd. executive said at the time that IoT vendors "need to do a better job of securing their devices, and from a regulatory standpoint, we need to do a better job of putting regulations in place to ensure that." Depow and Palazzo acknowledged that the advent of 5G will only introduce more threat risks that need to be mitigated.

The ISCC first registered to lobby the federal government early last year to boost its brand, profile and messaging, which is to maintain an open internet. At a conference preceding its registration, then-president and CEO of the organization's global operation Kathryn Brown said "governmental efforts at control, self-serving business models, unilateral security communiques are not going to be successful" to advance the development of that objective.

— With reporting by Ahmad Hathout at ahathout@thewirereport.ca and editing by Anja Karadeglija at akarad@thewirereport.ca