Internet Society Canada Chapter's (ISCC)

Mitigating Consumer IoT Cyber Threats Project

Forum 1 Overview: Contextualizing the Threat in the Age of a Global Pandemic

Internet Society
Canada Chapter

TABLE OF CONTENTS

Context

In the time of a global pandemic, the internet of things (IoT) is bringing forth innumerable benefits to society from innovation in health devices, including sanitization robots to convenience in the home, at a time when so many of us must shelter in place. At the time of this initiatives first Forum on February 20th, there were only nine reported cases of COVID-19 in Canada with six in British Columbia and three in Toronto. It is evident that changed rapidly, impacting how people live and work if they are so fortunate to have a job. McKinsey had previously said that the economic impact of IoT could be as high as $11.1 trillion per year by 2025 with the chip design firm, Arm, forecasting a trillion connected devices by 2035.

These forecasts are now challenged by disruptions in supply chains, lockdowns, and worker redeployment to respond to COVID-19. The millions of dollars pumped into projecting employment change and economic growth by both government and company business intelligence units are now of little worth, thanks to COVID-19. Redeployment of workers in Information Technology (IT), from data centres to telemedicine in hospitals as an example, takes priority away from IoT deployment. It is yet to be seen whether the time spent at home, in isolation, will result in consumer spending increases on smart home devices and their use or that mass layoffs and economic concerns will decrease adoption. Forecasts have not only turned to dust, so too has the debate over work from home productivity. Necessity has forced a previously expected gradual transition to working from home into digital nomadic revolution in a matter of weeks. Nevertheless, while the growth trajectory in some IoT applications may have changed, the need has not, perhaps more than ever.

With coronavirus so contagious and hard to contain, it is safer to utilize remote means of interaction rather than human to human. Both in hospitals and the public, remote communication means that patients avoid transmitting the disease and health workers save time for simple tasks. This has cleared the way for robots and other automated technologies to assist in the global pandemic response. Robots are being used to disinfect rooms, communicate with isolated people, take vital information, and deliver medications and other items.

Self-driving ultra-violet disinfection robots, utilizing LiDAR's[1], are now shipping to several hospitals in China to help fight COVID-19. With ultraviolet light, these robots can disinfect and kill viruses and bacteria autonomously, effectively limiting the spread of coronaviruses without exposing hospital staff to the risk of infection. Furthermore, facial recognition companies have adopted the thermal imaging–enabled facial recognition to identify people with an elevated temperature at various screening points[2].

The likely long-term growth of working from home could provide growth opportunities for the device sector and offer many benefits to help individuals and families manage their work and

[1] AP News, Feb 26, 2020 https://apnews.com/PR%20Newswire/354aae0738073bc95331ee72a458cb50
[2] Nature Medicine, Mar. 27, 2020 https://www.nature.com/articles/s41591-020-0824-5#ref-CR8

personal lives. The crossover of personal online behaviour and devices with those for work nevertheless creates uncounted threat vectors. This is at a time when people are vulnerable, inviting bad actors to do bad things.

The Project

Mitigating cyber threats for consumers is now more than ever a critical area for policy implementation. With the proliferation of connected devices, organizations and governments around the world will be enhancing the development, consideration, and implementation of mitigation capabilities.

Through a Multistakeholder approach of facilitating dialogue among business and members of the IoT supply chain, civil society, academia, subject experts and the public, the Internet Society Canada Chapter (ISCC) is pursuing much-needed dialogue in this critical area of importance to all citizens in today's ultra-connected world. Leveraging the Internet Society's Canadian Multistakeholder Process on IoT Security, this Project is building awareness and education to stakeholders in a way that changes behaviour and strengthens public policy to support public safety.

ISCC's Mitigating Consumer Cyber Threats Project is aimed at enhancing and maintaining intensity in knowledge sharing on IoT cybersecurity risks and solutions. With participation from subject experts in Canada and our closest allies, this Project will continue on that path through domestic and cross-border knowledge exchange.

The ISCC wishes to thank the British High Common in Ottawa for hosting the event. The ISCC is also indebted to our funding partners, the U.S. Embassy in Canada and Amazon Web Services; supporting partners, CyberNB, the Australian High Commission, Canadian Cybersecurity Threat Exchange, the CIO Strategy Council, U. Group, TwelveDot, Serene Risc and the Security Partner's Forum as well as the Mitigating Against Consumer IoT Cyber Threats Project Steering Committee.

The Approach

On Thursday February 20th, 2020, the ISCC organized the first Forum in its Mitigating Consumer IoT Cyber Threat Project. At that time, there were nine reported COVID-19 cases in Canada. As the world followed the growth of the pandemic, that number grew to over 9,000 by April 1st.

Introduced by Franca Palazzo, Executive Director of ISCC and Co-Chair of the initiative, the British High Commissioner, Susan le Jeune d'Allegeershecque, welcomed participants. The Forum had three panels, all with the objective of Contextualizing Consumer IoT Cybersecurity Threats: 1) The Perspective of the Consumer, 2) The Perspective of Business, and 3) Geo-Political Factors.

After the British High Commissioner's welcoming, introductory remarks were provided by Jonathan Fried, Coordinator, International Economic Relations and Personal Rep. of the Prime Minister of Canada to the G20. Promptly following Mr. Fried was a keynote address from Nazli Choucri of MIT. In addition to the three panels previously mentioned, further keynote addresses were given by Greg White of the University of Texas San Antonio and John Weigelt of Microsoft.

The first panel was "The Consumer Perspective," with lead discussants Sriram Gopal of the Association of Home Appliance Manufacturers, Laura Elan of CSA and Dr. Greg White from the Center for Infrastructure Assurance and Security, University of Texas San Antonio. The second panel was "The Business Perspective," with lead discussants Robert (Bob) Gordon of the Canadian Cyber Security Threat Exchange, Rene Breyel from AIOT Canada, Susan Pullar, Office of Home Affairs, Australian High Commission, Mary Jane Dykeman of INQ Data Law, and moderated by Faud Khan of TwelveDot. The third panel was "Geo-Political Factors" with lead discussants Tammy Schultz of the U.S. Marine War College, Alicia Wanless, PHd Researcher, King's Centre for Strategic Communications in the UK, Keith Jansa from the CIO Strategy Council, Emmanuel Kamarianakis of Global Affairs Canada and moderated by Jeremy Depow, Co-Chair, ISCC Mitigating Consumer IoT Cybersecurity Threat Project.
The objective of this report is to summarize the insights that were consistently recognized throughout the day. Rather than organizing these insights in the chronological order which they were discussed, the insights have been organized in such a way to aid in the readers' understanding of the Mitigating Consumer IoT Cyber Threats Project. These insights begin by discussing what cyber-attacks and threats are, transitions to how they affect society at large and concludes with potential solutions and next steps. It is worth noting participants of the forum are largely anonymized to promote freedom of idea sharing.

Insights

Cyber Attacks are a Threat to Both Public and Military

Cyber-attacks are putting organizations out of business.

Discussants widely accepted the notion that if a device is connected to the Internet, it is a target.
Infrastructure is a substantial risk, but people working in this area seem to have a better idea of the threat. Consumers, however, may not understand that there is a risk when they buy a smart home assistant or other device and put it in their office where they are having confidential meetings or in a very private space of their own home. The same goes for embedded cameras that can be compromised. There have been many examples with ring devices and child monitoring, only to find that bad actors and predators are using security vulnerabilities to their advantage.

Experience from the Canadian Cyber Threat Exchange, which has 135 member organizations, shows high business concern, particularly from organized crime. As a result of this organized crime, hacking has become a commodity and the IoT is now weaponizable. Moreover, the barrier to conducting attacks is coming down. For example, 84 percent of everything in a building is connected to the Internet. Small companies are just as vulnerable as larger companies simply because they are connected. The same can also be said about sole individuals running a business who often have a false impression that they are not a target. An attack could be motivated by many things, from anger to leapfrogging to another target. Cyber threats are "the great equalizer" for businesses of all sizes. On the ground experience has shown presenting good business ideas to privacy lawyers well past the conceptualization stage, illustrating a lack of security and privacy by design.

The impact on business is staggering when observing recent statistics from the United States. This data indicates 20 percent of organizations are reporting cyber-related business interruptions, of which 25 percent declare bankruptcy and 10 percent end up going out of business. The scale and number of attacks occurring in the market demonstrate an imperative to move forward now. Cyber incidents rank as the most critical business risk globally in the *Allianz Risk Barometer* for the first time in 2020. Seven years ago, it ranked only 15th with just 6 percent of responses if looking at the risk barometer—cyber number one, not number 2. The World Economic Forum has reported similar trends in its *Global Risks Report*.

In market experiences show that health care institutions train their workers, and just after anti-phishing education, most workers still fall for white hacker phishing. Several IT departments within the organization remain unsupported. Strengthening communication ability with executives and Boards may have a positive impact with simple techniques such as explaining previously thwarted attacks with improved descriptions of what those attacks look like to CEOs. In the past, a typical response, in the hospital community, to IT departmental requests for resources to mitigate cyber threats was to simply buy more insurance. Insurance clauses, however, are often dependent on the hospital's compliance with standards and have limits on what is covered. In Ontario, hospitals have a $30M cap on what is insured. Nevertheless, cyber threats are not only a risk to businesses and healthcare. These threats and attacks occur on a Militaristic level as well.

Offensive military cyber operations can backfire and invite attacks.

As articulated in the Geo-Political Panel, new norms are being created by the U.S. Government and other actors that will have ripple effects across cybersecurity. These changes came from the 2018 cyber strategy brought forward by the Trump administration as well as the still classified, even to the U.S. Congress, National Security Presidential Memorandum 13. These changes can be broken down into three categories:

The Militarization of Cyber

U.S. Cyber Command is now on par with combatant commands such as StratCom and CentCom, which are functional organizations. A combatant command is led by a four-star commander. The FY 2020 budget for the U.S. government allocated approximately $18 billion towards cyber. The Department of Defense received 55% of that budget, equaling approximately $10 billion.

Cyber Operations are Going Offensive

U.S. cyber strategy has shifted to persistent engagement and defending forward. Persistent engagement ensures that the United States is in cyber all the time, everywhere while defending forward revolves around the idea that the U.S. are going to confront threats in their respective lands, so they do not have fight on their own land. This means that the U.S. are always operating outside its own networks to stop cyber threats. Theoretically, before they hit the United States, the usual suspects of North Korea, Russia, China, and Iran have been primarily targeted. U.S. officials have described cyber operations in the context of being the same as the air force. Aircraft fly every day, conduct flying missions, provide warning of incoming threats, and provide a show of force for some time. Cyber operations are considered within the same concept that the U.S. does not wait for something to happen. In other words, deterrence theory remains to be the norm in the U.S. Department of Defence.

One discussant found the U.S. cyber strategy puzzling as the Department of Homeland Security (DHS) is the federal agency in charge of protecting federal government cybersecurity and protect information from leaking out of the private and public sectors as well as local and state levels for cybersecurity. Therefore, it remains to be known why the DHS is not the primary driver of U.S. cyber policy. While the 2018 cyber strategy pays lip service to protecting consumers and private/public sector cooperation, the funds are flowing elsewhere.

No Longer to be Treated Reactively

The third major departure comes directly from the cyber strategy, which essentially says the cyberspace is no longer to be treated reactively. Previously, there were questions of if an attack was not kinetic but rather cyber, taking out power grid that resulted in death, what military options did the U.S. have? This was an open question. The 2018 cyber strategy says the U.S. military could respond through multi-domain warfare or what is increasingly known as hybrid warfare.

It was brought up that the Five Eyes (FVEY) alliance, consisting of Australia, Canada, New Zealand, the United Kingdom and Unites States, is under threat after the U.S. Ambassador to Germany tweeted if a FVEY ally uses China's 5G technology, information and intelligence sharing would be compromised. FVEY has been in existence since 1941.

Cyber threats go beyond simply malicious attacks to an individual, business or military. They can be used to gather strategic data, personal information, or to influence a group of individuals to act a certain way.

There are a variety of tactics, in an IoT world, used to influence a target audience with information.

There is relevance in how information is used to influence the target audience, particularly when those actors are in competition or conflict to exert their will on each other. This includes a variety of tactics by extracting information and how that is used against targets or pushed out to gain attention. Influencing information involves a complex system that includes the infrastructure, software, data, but also human condition. Understanding the information environment concerning competition, and that the factors that give different actors advantage over each other are essential to combat the negative consequences.

Given the complexity of interconnected devices' information systems and a variety of tactics used in information influencing, it was suggested that the subject be examined in a broad context. Data from multiple sources, including connected devices, is aggregated to develop intelligence on an adversary. An example of the previously mentioned scenario could be military personnel, using fitness trackers and then a company taking the data from its customers and using that to market their more extensive reach. This example may seem innocuous until on realizes most people using fitness trackers in a country like Afghanistan are military personnel, which thereby gives up vital data around a military basis.

Another area of information which can be used in an IoT context is the targeting of critical people. Common connected devices like a cell phone offer a wealth of data that could be used against a target, not the least the data and messages related to what is on that phone. There are "layers" on a smartphone that makes protection more complicated. Not only does an individual have contacts, photos, and personal messages, but also software from social media accounts linked to the aggregation of more data on this target putting the individual at even greater risk. Furthermore, smartphones can also be used to control other IoT devices such as laptops or SmartTVs to name a few.

The term IoT can give the impression that devices are devoid of humans; however, behind all devices are people who develop, manage, and use the technology. Furthermore, the users are the most critical link. The fact is that considering how humans both use and abuse technology inadvertently and deliberately for influencing purposes needs to be front and center. Commercial mindset often prioritizes what a product solves and its unique selling proposition. What can be missed is a company's consideration of how an IoT product can be abused or used in different ways than intended.

Geo-Political Factors

Multilateral cyber warfare disarmament treaties may be influential mechanisms to mitigate threats to citizens.

United Nations Secretary-General António Guterres has made a peaceful Information and Communications Technology environment one of his key priorities. In May 2018, the Secretary-General launched his Agenda for Disarmament[3], where it is noted that "global interconnectivity means that the frequency and impact of cyberattacks could be increasingly widespread, affecting an exponential number of systems or networks at the same time." and that "in this context, malicious acts in cyberspace are contributing to diminishing trust among States." To address these challenges, the Secretary-General has included two action points on cyber in the implementation plan of the Agenda for Disarmament[4]. These action points are as follows:

- The Secretary-General will make available his good offices to contribute to the prevention and peaceful settlement of conflict stemming from malicious activity in cyberspace.
- The Secretary-General will engage with Member States to help foster a culture of accountability and adherence to emerging norms, rules, and principles on responsible behaviour in cyberspace.

The G20 represents nearly half of global Internet users, and the digital economy continues to be a present priority for the Group's participants and leaders. Several countries have provided proposals and ideas through several multilateral bodies regarding Internet governance. During the 2019 G20 summit in Osaka, Japan, leaders underscored the importance of a secure Internet, including IoT.

The various matters under discussion in the international community involve consumer digital education, empowerment, redress (*possibility for individuals to obtain damages for breaches)* across borders, and digital trade. Yet, much of the dialogue is heavily politicized with countries acting to favour their own social, economic, and political interests. Policy on IoT cyber security standards is an example of intense politicization. This international relations reality-check adds to the value of multi-stakeholder policymaking.

Digital ministerial meetings further issues such as consumer digital education, empowerment, redress across borders and in other areas. Several countries have put forward ideas in varying for an including in the United Nations. Countries like Saudi Arabia are active on digital issues, which is prominent. It was expressed that countries are using their influence with the

[3] United Nations Agenda for Disarmament, May 24 2018, https://www.un.org/disarmament/sg-agenda/en/
[4] United Nations Office for Disarmament Affairs, Dec. 2018 https://www.un.org/disarmament/ict-security/

International Telecommunication Union (ITU) to develop standards that favour social, economic, political interests, and that this is outside ITU's traditional competence.

Trade is also affected and has prompted efforts by the World Trade Organization (WTO) and is recognized in the United States Mexico Canada Agreement. Thus far, eighty countries have signed on to the WTO with the goal to have all 164 countries to sign on. The efforts are for continued expansion of digital trade.

Many countries are trying to evolve and conform through bilateral and multilateral means. There are fundamental differences, however, between Russia, China, the U.S., and the EU on the role of the state in regulating the digital economy. This leads to a need to prevent the risk of Internet balkanization.

Issues being addressed are international data flows, online dispute resolution systems, consumer empowerment, and redress across borders. Several countries have put proposals forward.
There is support for a free open, interoperable Internet that supports inclusive growth. Canada is taking a holistic approach so that consumer product safety and redress can be coordinated internationally. Strong support was given for multilateral approaches.

Given the very different values and perspectives among societies as well as the new norms in cyber warfare that are primarily creating chaos, the concept of warfare disarmament treaties was brought forward. This is especially a topic of interest given the transfer of the cyber warfare domain to kinetic activity.

It was generally agreed among participants that the threats of cyber warfare are of high consequence, including resulting in military and civilian casualties either directly or indirectly. It is therefore, of importance, to consider consumer IoT cyber threats on the same level as a nuclear or chemical weapons. As such, using previous disarmament treaty development process for the cyber warfare domain may be of positive impact in mitigating threats to citizens.

Lessons from Australia.

In Australia, cybersecurity sits in the Australian Home Affairs portfolio of what the Australian government is doing in terms of cybersecurity and IoT. In the context of the 2019 Australian federal election, there was a promise to have a best practices guide. The IoT Code of Practice[5] is Australia's first significant step. Australia has 64 billion devices to be connected by 2025 and want to see the benefits. As has been documented, Parliament House experienced a

[5] Code of Practice, Mar. 30, 2020 https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/code-of-practice

significant cyber-attack during the lead up to the election. Therefore, the security of the economy is paramount in Australia.

The Code of Practice targets an industry audience with voluntary principles and signals to the market that all internet-connected devices should be secure by design. While the Code targets an industry audience, consultations with the public are taking place about meeting their needs. Public workshops and forums in every state in Australia support that input. Industry is a key partner with the role of protecting consumers and securing the nation. The Practice has 13 principles and putting the first three principles in priority sequence as the most important. These three principles include:

1. No duplicated default or weak passwords
2. Implement a vulnerability disclosure policy
3. Keep software securely updated

These principles are explained in further detail, along with the other ten principles, within the Code of Practice. The Australian government is committed to voluntary principles and would only change if that proves ineffective over a length of time.

Encryption is an essential discussion in Australia. As such, the country has passed legislation that the government supports encryption but also allows for specific agencies to have access. They are not asking for back doors but instead are asking providers to assist. Consultations have been released and are currently on the Home Affairs website. More will be added as consultations are completed. The importance of standards being globally consistent is a key take away from the experience.

Public Policy Engagement

Multistakeholder and consensus building approaches to mitigating consumer IoT threats are "what count".

Multistakeholder participation is a governance approach where multiple relevant stakeholders participate in the collective shaping of policy. Multstakheholderism is widely used in Internet Governance. It was noted, throughout the day, that it is important for governments and citizens to be sharing ideas and best practices among allies given the multifaceted nature of the challenge and perspectives needed from business, academia and governments to mitigate IoT threats. This approach is described as "what counts," in mitigating consumer IoT cybersecurity threats.

As largely elected officials, legislators rightfully represent jurisdictions with multiple interests across our respective countries. Most citizen legislators are generalists with a mandate that covers many issues citizens face. If not appropriately articulated and grounded in a legitimate

multistakeholder process, consensus standards and other threat mitigation efforts may be interpreted as purely industry-driven and not open.

Global technology companies and smaller manufacturers are critical to deployment, user interfaces, the supply chain and innovation. If coming from an area of mistrust, however, education and explainable examples of compliance requirements can help build trust among all stakeholders in the policy ecosystem.

Civil society is not yet fully engaged in IoT security public policy discussion.

One discussant articulated how civil society is helpful when it articulates its expression of its interest. So far, it was observed that civil society, a critical component of a correct Multistakeholder approach to cyber challenges, have been mostly silent.

Civil society is an aggregation of many interests. While caught between many rocks and hard places, civil society has the potential to meet the demand for better security despite being somewhat inactive in the cybersecurity realm. Public discourse has been dominated by tech suppliers and is further complicated by a lagging voice from governments who have come into the discussion much later. This results in little movement on regulatory mechanisms from civil society, for example, and the lack polarization is perhaps a signal of non-engagement. The bottom line is to help civil society is to help the consumer.

Civil society's role in supporting consumers can assist with answering what supports society and consumers need with technology advances concerning IoT. Facilitating civil society engagement must be done in a manner where they are not, however, barraged by information to digest if IoT security is not their central area of focus.

A challenge identified is the lack of hands-on training for students. This prompted the development of programs such as CyberPatriot, now implemented in four other countries, including Canada, to provide introductory hands-on training. Competitions such as CyberPatriot provide unpredictable real-life scenarios that include not only technical but legal, business, and customer implications.

Activities such as CyberPatriot assist with the need for citizens to be prepared mitigate threats. Multiple efforts must be taken to contribute to a pervasive culture of security at the community level. Reference was made to the 90 percent identification rate for Smokey Bear and 80 percent for McGruff the Crime Dog. Smokey Bear, the U.S. Forest Service's symbol of fire prevention, is the longest-running public service ad campaign, first appearing on a poster on Aug. 9, 1944.

CyberNB has created a Cyber Immunization program for K – 6 students, with a focus around central characters; Cybear, Reverse and Malware. The comic was designed with input from students and a second edition will be available shortly. All content is in English and French,

with teacher kits developed that will allow teachers to have discussions with students around online security, cyber hygiene, smart decisions and understanding the key concerns and risks to online activity. This curriculum is anticipated to cross Canada in the next year and become more familiar with students. Eventually, to be recognized by students and parents alike similar to Smokey the Bear.

Standards as Pivotal to the Solution

Battle Royale: Standards play a pivotal role in mitigating IoT cyber threats, yet the standards development environment is rife with competition.

The Forum was not only an event to share and inform. A healthy debate on standards development and effective solutions to cybersecurity were also a large component. There are many cybersecurity standards related to IoT that are in continuous evolution. These standards are developed by a variety of organizations, including private sector enterprises, civil society, the International Telecommunications Union, ISO, NIST, ISC, ITF, ACP World Economic Forum, United Nations, and World Trade Organization. The standards development environment is rife with competition among enterprise, social, economic, and political interests.

The role of manufacturers and service providers can be a challenge since individual companies have their idea of what adequate protection should be. This dynamic creates a great deal of competition in areas such as standards development as organizations maneuver to have their goals achieved through these mechanisms. This competition creates an environment where it is challenging to develop an industry position on how privacy is defined.

Nevertheless, whether related to networks or cybersecurity products and processes, these standards can be highly similar where best practices can be distilled down from the vast body of information available. Standard-setting body versus another story versus different industry groups. Quite frankly, it is not the standard that is as important as the process for which it has been developed.

Standards are not a one size fits all.

Participants referred to the multitude of standards bodies specific to IoT (some referenced above) as well as the numerous indirectly related certifications and regulations such as the Electrical Safety (CSA, Grid Code), Health (Medical Device Certifications, Software as a Medical Device), Transport Canada (drones, personal vehicles), Measurement (Weights and measures), Safe Foods Regulations, and the Canada Consumer Product Safety Act which includes helmets and smoke detectors.

There are different ecosystems, such as in food packaging or transportation, at play with factors that need unique consideration such as the economics of IoT products and services

(how companies make money) and the user interface or customer experience. Each case may have individual needs.

One discussant brought up improvement needed in guidance, including:

- Greater recognition of the continuum of devices
- Address alternative modes of remediation (disposal, recall)
- Include an ecosystem approach (Managed security providers, smart hubs, Etc.)
- Better define roles and responsibilities (Hardware, OS, App)
- Address existing certification requirements (Health, Energy, Safety)
- Closed vs open networks (OT vs IT) (e.g. home security)
- Explicitly call for Security Development Lifecycle (e.g. ISO 27034)
- Responsible tech development practices
- Inter-IoT device communications
- Accessibility
- Modes of operation
- Modular Design (abstract out the controller from the mechanical)
- Need to address consumer safety (either in scope or out of scope)
- Redundant sensing, n-version programming, fail-safe, no false negatives

Supporting supply chain and manufacturers with consensus standards.

Security features should be programmed into the device, with the help of consensus standards that are agile enough to be updated. While the multistakeholder, consensus-building standards models is still a slow process, they are not as protracted as legislative implementation.

The manufacturing community, who also has standard development bodies, articulates the division of the IoT policy universe into three key buckets: 1) safety, 2) cybersecurity, and 3) privacy, all of which interrelate. These buckets touch on protecting the integrity of devices, network privacy and consumer data. It was noted that the community of manufactures that are not familiar with IoT security methods need to be brought into the fold to follow through the security life cycle for software and achieve greater recognition of the continual of devices.

A platform to address fragmentation in standards may be a valuable tool for consumers and businesses.

Sharing data among allies is a useful practice in multiple forums. A tool that addresses fragmentation in standardization, given the competition in the field and varying values, could be a valuable tool for stakeholders.

As an example of the critical need for action, one discussant explained how medical devices provide data insecurely; there is no encryption. In undertaking vulnerabilities check, minimal

efforts were taken to capture data. Moreover, third-party vendors have access through back doors to assist their clients remotely. Tools that assist in providing awareness of risk levels and clear methods to utilize standards to address such risks have been highlighted as in demand.

Careful consideration must be taken into what can reasonably be expected from consumers and over-reliance on individual responsibility.

While the concept of shared responsibility in liability was generally accepted, there was general concern over an unrealistic expectation placed on consumers. One discussant suggested that the consumer is the most neglected, and there may be an underestimation of the burden placed on consumers to mitigate IoT cybersecurity threats in a supply-driven environment. In such an environment, security by design is lacking. COVID-19 has demonstrated that citizens often do not take threats seriously, even when given clear guidance to protect their health and safety. Disobedience with guidance in COVID-19 makes it clear that consumer cyber education will have minimal effect on its own, and there is need for balancing individual responsibility with ensuring security by design and a robust mitigation ecosystem.

There is a dilemma that most individuals who are responsible for Internet Governance come from a time when the Internet did not exist. Furthermore, the responsibility to set up the norms for future generations also lies in their hands. This dilemma contributes to a rapidly changing world which people are trying to understand. As previously mentioned, consumers are one of the most neglected aspects of the cyber world and cyber realities. There should be caution in thinking of the consumer as only someone that buys something. Consumers are also a voter and have the capacity to have a global voice. Individuals are exposed to new possibilities and threats, facing challenges to manage all of this effectively, as non-experts. It was also put forward that personnel must respond to consumer demand for education and help.

There are multiple perspectives on the responsibility of citizens for their safety. The example of Hawaii's law of requiring all citizens to have seven days of supplies in the event of an emergency provides an analogy for the responsibility of individuals. As one discussant stressed consumers, businesses and governments must undertake simple tasks and have the responsibility to do so, such as to back up, back up, back up.

The password is a security measure of the past.

In the absence of federal incentives, some states are taking an active role in developing cybersecurity laws in frameworks, driven mainly by California. Other states taking an active role include Oregon, Vermont, Washington State, Virginia, Maryland, Texas, New York, Massachusetts, and New Hampshire. There are now 11 states that have either passed or considering cybersecurity laws.

A problem that has been brought forward with these laws is that they often say each device put on the market requires a unique password and must conform to reasonable security measures. The password is a security measure of the past and is no longer relevant to today's world. Even with a unique password on each device, the consumer then must change to their password. It is well known from human behaviour, however, that most people use two or three passwords for multiple purposes.

This is not suitable mitigation given technology is connected in some way, and how humans act and share data lessens the value of passwords. IoT involves everything from medical and consumer devices to industrial control devices. The "smart" products consumers carry around today are connected to our homes and buildings through wired or wireless networks using many different technologies protocols.

Manufactures must design security into devices at the outset to account for a supply-driven environment.

There is a need to balance the provision of educational materials for a consumer device with the building in of design mechanisms by manufacturers. Design security into devices at the outset translates to not only a focus on consumer education but also for product innovators, meaning a conversation about approaching the entire ecosystem. Labels are in the equation; however, even once labels are in the market, it took previous labels several years to sink into the marketplace. Therefore, consumer education is going to take time.

Solutions can involve physical separation of safety controls from the Internet. One discussant brought up the example of physically separated safety limiters, in ovens, for any component that can connect to the Internet.

Meaningful consent may not be possible in a "terms and conditions" format

A big challenge for civil society and consumers in general is understanding what meaningful consent is and that it may not be possible to be achieved in the context of a terms and conditions agreement. Questions arose on the value of what General Data Protection Regulation brought forward by forcing a website to request users to accept cookies. It was noted there are few in market frameworks that elicit meaningful consent from the customer rather than just a simple accept cookies button.

Discussants debated over the ability for consumers to protect themselves, given broad behaviours that they are not going to do what they are supposed to do. The analogy, not so distant from required government efforts in response to COVID-19, is regarding the introduction of the seatbelt. Despite instruction for all cars to have them and passengers to wear them, it took enforcement through tickets to ensure compliance. In other words, people simply, at a basic behavioural level, often do not do what is mandated. A culture of Internet security, almost like a culture of social distancing, is what is required.

Information Sharing Operation Centres are of high value to mitigation efforts

Of relevance are the use of Information Sharing Operation Centres (ISOCs), that exist across the United States and have been introduced by the Canadian Cyber Threat Exchange and CyberNB. Many Canadian enterprises, including those in the electricity sector, belong to bilateral ISOCs such as the North American Electricity Reliability Corporation. The threat response and trust-building capabilities of well-structured ISOCs are of high value to mitigation efforts. More countries are wanting to create ISOCs.

CyberNB has entered the third year of its project for collaborative security operations in critical infrastructure. Known as the CI-SOC, participants to date include major cybersecurity service providers, critical infrastructure operators and government agencies. The CI-SOC is developing maturity models, mutual assistance programs between partners, and new data sets for advanced analytics to ensure threat is identified earlier. Additional outcomes are anticipated to include new standards and operational maturity models, as well as support supply chain safety in critical infrastructure, supporting the industry driven "Charter of Trust" that is led by multinationals such as Siemens.

It was also agreed that countries should be encouraged to share domestically as that will make it easier internationally and allow U.S. to build trust. Much has been done internationally with allies in forums such as the FVEY alliance. The level of sharing in FVEY is enormous, following and sharing on election issue prevention. An attack in one organization may affect another. Currently, Industry does not know where to look for a trusted resource should an incident occur or for prevention. This is a necessity.

Information sharing and operations centres can exist at multiple levels and sizes, including for community cybersecurity models. It helps a community start a cybersecurity program even at a basic level where there is minimal funding. A community can look at their economic profile to determine where they need to focus. San Antonio, for example, has a higher target potential for multiple reasons such as NSA Texas, 16th air force, and tourism

Contrarily, if something happens in a state like Hawaii, it is going to take days to amass a physical presence there. Unlike Texas, Hawaii cannot depend on rapid response. In Hawaii however, citizens are expected to have enough emergency supplies for seven days. Individuals have a responsibility for personal safety. Texas does not have this regulation. The bottom line, Hawaii understands. When thinking cyber, each nation must think the same way. Communities are a target. If the technology is there and it is connected, it is guaranteed to be a potential target.

Federal organizations have learned much has to be done at the community level, given the relationship between communities, their businesses and critical infrastructure. One discussant

highlighted that information sharing was doomed to fail without an underlying cybersecurity plan at the community level. However, information sharing, and cybersecurity plans are not only a priority on a domestic level. Recently, these issues have become significant topics of conversation on an international level too, albeit for very different reasons.

Conclusion

In a time of uncertainty due to the COVID-19 global pandemic, the internet of things (IoT) is bringing forth innumerable benefits to society from innovation in health devices, including sanitization robots to convenience in the home, at a time when so many of us must shelter in place. Mitigating cyber threats for consumers is now more than ever a critical area for policy implementation.

As the insights collected from the first forum of the Internet Society Canada Chapter's Mitigating Consumer IoT Cyber Threats Project indicate there is a complex multi-vector threat to consumers that must be continually addressed so the benefits presented by these tremendous technological advances can realized for society.

Civil society has perhaps been less engaged in this subject matter, however, however recent events including the utilization of contact tracing applications to confront COVID-19 is forcing greater involvement.

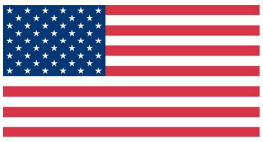
The policy landscape is as complex as the technologies themselves. Through information sharing among stakeholders, mitigation efforts are being strengthened. ISCC looks forward to the next steps of our Mitigating Consumer IoT Cyber Threats Project and building on the first forum to dive deeper into effective solutions through Multistakeholder involvement and working closely with our closest allies.

Author:

Jeremy Depow
Co-Chair and Special Advisor, ISCC Mitigating Consumer IoT Cyber Threats Project

Internet Society
Canada Chapter

THANK YOU TO OUR FUNDING PARTNERS



EMBASSY OF THE
UNITED STATES
Ottawa, Canada

aws

AND SUPPORTING PARTNERS

British
High Commission
Ottawa

CIO
STRATEGY
COUNCIL

SPF
SECURITY PARTNERS'
FORUM

Australian
High Commission
Canada

CYBERNB
SPECIAL OPERATING AGENCY
ORGANISME DE SERVICE SPÉCIAL
ONB

U.Group

Canadian Cyber
Threat Exchange
Informing Canadian Business

serene
risc

TwelveDot

internetsociety.ca

@ISCC_Canada internet-society-canada-chapter