Statement of Joshua Corman

For the House Oversight and Government Reform Committee's Subcommittee on Information Technology "Cybersecurity of the Internet of Things"

Oct 03, 2017

Opening:
Chairman Hurd, Ranking Member Kelly, and distinguished Members of the Subcommittee on Information Technology, thank you for the opportunity to testify today.

My name is Joshua Corman. At the time of writing this, I am the Director for the Cyber Statecraft Initiative in the Brent Scowcroft Center on International Security at the Atlantic Council – a non-partisan, international policy think tank. I am a Founder of "I am The Cavalry" (dot org) a grass roots, volunteer, cyber safety initiative focused on public safety and human life in the internet of things – or as we like to say: "where Bits & Bytes meet Flesh & Blood". Additionally, I am an adjunct faculty for CISO Certificate Program at Carnegie Mellon University's Heinz College where I've worked with dozens of CISOs at a time. Lastly, I testified to the *2016 Presidential Commission on Enhancing National Cybersecurity* and served on the *Health Care Industry Cybersecurity Task Force* – initiated by Congress in the Cybersecurity Act of 2015.

Over the past 16 years, I've been a staunch advocate for the role of CISO (Chief Information Security Officer) – an increasingly difficult role. A significant portion of my research and career has been focused on the vanguard of emerging threats, and challenges affecting cybersecurity as well as identifying, advancing, and originating new and more effective responses to these growing challenges. As such, I've worked deeply with many of the Fortune 50, 100, and 1000 – on emerging issues such as the rise of cybercrime, the rise of nation state espionage, the rise of Anonymous & hacktivism, the Cyber Caliphate, and the growing exposures to cyber safety and national security as we become increasingly dependent on the Internet of Things.

As we continue to misidentify cybersecurity as primarily about the confidentiality of data, we grossly underestimate the urgency the situation commands. Over the last 2 years we are trending toward high consequence failures – well beyond data. As the most connected nation, we stand the most to lose.

Through our over dependence on undependable IT, we have created the conditions such that the actions of any single outlier can have a profound and asymmetric impact on human life, economic, and national security.

"I am The Cavalry" created this over-simplified list of material differences across the various types of IoT. Differences in:

- *Adversaries*: Motivations, Objectives, Capabilities, Will
- *Consequences of Failure*: Life & Limb, Physical Damage, Market Stability, GDP, International and National Security
- *Context & Environments*: Operational differences, Migratory, Perimeter-less, Inaccessible, Difficult to Patch/Replace
- *Composition of Goods*: Hardware, Firmware, Software
- *Economics*: Margins, Buyers, Investors, Costs of Goods, Regulatory, Depreciation
- *Time Scales*: Time-to-Live (TTL), R&D Cycles, Response Times

It is worth noting that Cybersecurity is a relatively nascent field – and is having a very difficult time rising to meet the challenges. High profile failures in the private sector and in governments are becoming quite clear. About 100 of the Fortune 100 have lost intellectual property or trade secrets to foreign industrial and nation state adversaries. Most Merchants have had a breach of credit cards – despite being compliant with "best practices" and industry compliance regulations like PCI DSS (Payment Card Industry Data Security Standard). Breaches are getting bigger like Target and Ashely Madison. Breaches are hitting Federal Agencies like the Pentagon and OPM. Breaches are getting dangerous as we connect everything in the Internet of Things – such as the denial of patient care at Hollywood Presbyterian Hospital in California due to Ransomware. WannaCry took out 65 UK hospitals – the US got VERY lucky. NotPetya hundreds of millions of dollars of damage to Mersk, Merck, and others. The Internet of Things is where bits & bytes now meet flesh & blood. In fact, the problem statement which caused me to form "I am The Cavalry" was:

"Our dependence on connected technology is growing faster than our ability to secure it – in areas affecting public safety and human life."

As society (and the government) increasingly depends upon IT, the importance of effective cybersecurity must also rise in kind. In the case of HHS, the consequences of failure may bleed into public safety and human life. We must be at our best.

"There are things the Public Sector ***can't*** *do, and the Private Sector* ***won't*** *do… and this is the role of Philanthropy and Altruism."*

– Eli Sugarman, Hewlett Foundation

As that 3rd category, I'm can say this issue has fallen through the cracks of the "Public Private Partnership" model.

Over the last 30 years, we have been *reluctant to regulate* software and IT. There are a number of concerns that have fueled this – some valid, some now less so, and some never were. The chief concern has been a fear that such actions might "Stifle innovation and hurt the economy." Attacks like Mirai launched from the long tail of low cost, low hygiene IoT device showed us that a *failure to regulate* IT can "stifle innovation and hurt the economy".

Since Mirai, we've seen significant damage to safety critical systems in the devastating impacts of WannaCry and NotPetya. A known but unmitigated vulnerability enabled WannaCry to take out 65 UK hospitals in a single day (20% of their national capacity of trusts) and affect manufacturing and other industries. NotPetya did material harm to Mersk shipping affecting the Port of LA, and Merck affecting their public earnings and having a material impact on their production of vaccines – like Hepatitis-C. Healthcare alone affects one sixth of our economy. Any crisis of confidence in the public could materially affect our economy. Any avoidable or elective shortfalls of our national supply of pandemic vaccines, the availability of life saving service during a natural disaster or domestic attack, or significant interruptions to critical infrastructure… could be devastating to our national interest.

What Mirai revealed:

DDoS attacks from the Mirai botnet took out the Internet for a good chunk of a Friday – affecting eCommerce, access to Netflix, CNN, Spotify, and other web services. It levied what was (at the time), the largest flood of traffic in history – at around a Terabit per second. Worse, only a fraction of the full botnet was leveraged in this attack – and those nodes participating only used a fraction of their possible sending capacity. At the time, I referred to Mirai as an IoT Tsunami of our technical and security debt catching up with us. The growing number of low cost, low hygiene IoT devices on the internet represents a public health issue for a reliable and sustainable Internet.

On a technical level, 3 things enabled Mirai to be so bad. These devices:

1. Were Internet reachable
2. Had guessable credentials (username & password) [and in this case fixed]
3. Were un-patchable

This combination is not isolated to the (majority) Internet Cameras. These said same 3 attributes apply to far too many medical devices – including $500,000 imaging equipment and devices that may directly harm patients. The next Mirai-like botnet could both target incredibly vulnerable hospitals to cause a denial of patient care – or actually be *comprised of* unfixable medical devices. Other, legacy critical infrastructure shares such attributes in Oil & Gas, Power, Water, and other designated US Critical Infrastructure

Uncomfortable truths command uncomfortable responses. If we want to see something different, we need to incentivize something different.

We have technical solutions for many of our exposures. What we have previously lacked is motivation and will. I am hopeful that the Senate Bill and this hearing are signs this is changing.

From a policy perspective, Mirai disrupted the "prior prevailing hopes" with regards to lighter touch regulation/policy. Prior discussions were focused on the belief that adding transparency, security "nutrition labels", and a software bill of materials (or ingredients list) that would enable consumers and purchasers to better discern "more secure products" from "less secure products". The bulk of discussion was about enabling free market choice. Mira revealed the externalities challenges and Tragedy of the Commons aspects of our inter-dependence. While transparency can allow each of us here today to buy a safer product, choices made *by others* can still hurt us – severely.

As someone *from* the Software, IT sector, and security research community, my natural preference to let the free market regulate itself – where informed, self-interested "demand", meets sufficient "supply". The 2 main areas where free markets – on their own – tend to need help are when there is either:

1. "Information Asymmetry" - where buyers lack enough information to act in their own self-interest, or

2. the rarer, “Tragedy of the Commons” – where even if each of us act in our own self-interest and local optimums, the whole is harmed.

Mirai and other cybersecurity issues are showing us we have both. The general fix for Information Asymmetry is to require more labeling, information, and transparency – to be *descriptive*. The fixes for Tragedy of the Commons is often using either *ex ante* (prior to harm) more *prescriptive* “what to do” requirements, or *Ex Post* (after harm) liability for outcomes – without prescribing *how* to avoid said outcomes. The rate of change in IT make *ex ante* too brittle to have efficacy over time and are more likely to stifle innovation or introduce barriers to entry for smaller players (or new entrants).

On S. 1691:

Initial exploration of what became Senate Bill 1691 appears to have followed the uncomfortable truths revealed by Mirai – and continued to evolve in the face of other critical mass in the policy community (see Critical Mass section below).

In broad brushstrokes, it is a technically grounded set of evergreen “Cyber Hygiene” principles that should be reasonable, achievable, and effective for classes of accidents and adversaries. High intent, high capability adversaries will remain an issue, but these principles should significantly raise the bar.

NOTE: The senate bill alone will not prevent the next Mirai. I believe they know that. Nor are large scale IoT denial of service attacks the only risk. Poor hygiene IoT could be at the root cause of the next OPM or Pentagon breach – or attempts to surveil or compromise your own Congressional offices via your Smart Television or Smart Gadget (for example).

These procurement guidelines may set an example for the private sector to adopt broadly, and/or a Self-Regulatory Organization, and/or international response (See International section below). In the face of a high consequence failure, I would not be surprised to see case law or introduction of software liability – and this rubric could inform and contribute to something like “safe harbor conditions” around “known vulnerabilities”.

On Known Vulnerabilities:

All software has flaws and nearly no software will ever be without vulnerabilities (in any scalable, economic way) so we have to prioritize. “Known vulnerabilities” are a key chunk of an 80/20 Pareto Principle here. Known Vulnerabilities are significantly more likely to be exploited than unknown ones. For example, the vulnerability is BASH that enable ShellShock had been there for 2 years, but was not attacked (broadly) until discovered. Once a vulnerability is known, there is a gold rush effect (or a shark frenzy with blood in the water) where adversaries and defenders create methods of finding and exploiting them – fairly quickly.

Broadly speaking, the talent required to *find* a new vulnerability can often be high. The talent required to *create a reliable exploitation* of vulnerability can also be high. Once an attack tool is created and shared, using these tools can be *executed by nearly anyone*. In the spirit of Moore's Law (describing the growth rate of computing power), I once coined a term called "HDMoore's Law" – in that the strength of an unskilled adversary grows at the rate of the Metasploit Project (a free open source attack tool used by defenders – created by security researcher: H.D. Moore). Later, a data scientist Michael Roytman showed how a Known Vulnerability CVE (Common Vulnerability and Exposure) in both Metasploit and the ExploitDB was 30 times more likely to be attacked than one that wasn't.

Further, it is far more reasonable to expect vendors to be responsible for avoiding or remediating known vulnerabilities than the bevvy of as-of-yet unknown, potential ones. In the case of 3rd party and open source libraries (which can be north of 90% of modern software composition) the remediation is often done by those projects and the fix can be applied by the final goods assembler with significantly less effort than fixing their own custom, bespoke code.

Senate Bill 1691, by expecting products to be free of known vulnerabilities as a condition of procurement, dramatically reduces elective risk. By requiring these known vulnerabilities to at least be disclosed, informs/supports them to assess, factor, accept, shield those issue in their purchasing choices and their operational security throughout deployment. The current opaque model constitutes a "failure to warn."

One short fall of this bill is the omission of a software bill of materials – of all the 3rd party and open source libraries used in the product (including version numbers). There have been negative reactions from parts of the private sector to such proposals – some of which have merit, many of which are false. I could explain some of these upon request. There is limited adoption of this in the private sector, but they are proving it can be done and has value. E.g. Philips Medical is voluntarily publishing a Software Bill of Materials to their customers – and some other medical device makers are starting to. Not to mention the concept was pioneered by Deming at Toyota in the 40's – to drive efficiency and profitable manufacturing. Carrots & Sticks could be explored – as well as a timeline for enforcement.

Here are at least three use cases enabled by the inclusion of such a Software "ingredients list" (the likes of which are required by all food, for example):

1. At procurement time, buyer can tell better hygiene products from worse hygiene product and/or or factor the cost of aftermarket securing them in their deployment uses (currently covered by S. 1691)
2. For the life of the deployment, when a new vulnerability becomes known, they can immediately answer 2 questions
    a. "Am I affected?", and
    b. "Where am I affected?"

    especially when time is of the essence and patches may not be available (This could have helped avoid the Feb 2016 hospital outage at Hollywood Presbyterian Hospital – which was due to 1 Java flaw - in 1 JBOSS library in - 1 device – and they were warned about it, but didn't know what might use it)
3. Since companies go out of business, and product support expires, there will be no alert notification or security update ever coming – and this list is your only way to triage and react

On Patching & Security Updates:
After Mirai, I said "Unpatchable IoT are the lawn darts of the Internet" – in that they are inherently unsafe – "unsafe at any speed"… Since all software has flaws, and new vulnerabilities will be fund and exploited, robust, reliable, prompt and agile updates are going to be table stakes. With great connectivity, comes great responsibilities. One can no longer be hackable, but un-remediate-able.

Commerce NTIA's process on IoT Patching and Updates could be leveraged here.

On Avoiding Fixed Credentials:
This was a key factor in enabling Mirai. Sadly, this is quite a common practice. While initial default passwords and the ability to physically (or locally) reset them do have use cases, there are many established practices to avoid *keeping* these password after installation. The collective harm of the status quo is too high (even if localized risk is acceptable).

On Non-Deprecated / Standards Protocols and Crypto:
There is value here as well – as too many vendors try to be clever in effective ways – or use available but ineffective protocols, technologies, and encryption.

We would not want to stifle emerging, but as-of-yet not Standard innovations like the next Bluetooth. Perhaps, like disclosing known vulnerabilities, the bill could require non-standard or old technologies to be explicitly declared.

On Coordinated Vulnerability Disclosure and Safe Harbor for Good Faith Research:
Many in the security research community were pleased to see another acknowledgement of the value of good faith security research. Laws like DMCA and CFAA have had a significant chilling effect on security research – research which can have profound benefit to the manufacturer, their customers, the public good, and public safety. E.g. recent fixes to medical devices like:

- the Johnson & Johnson ANIMAS Insulin pump (found by Jay Radcliffe), or
- the bevvy of Voting Machine flaws found during this year's DEF CON hacking conference (attended by your own Chairman Hurd and Rep. Langevin) to help ensure the integrity of future elections.

In 2015 and 2016, "I am The Cavalry" and others supported no less than 18 US Government positive actions related to the value of coordinated vulnerability Disclosure. Those included, FDA guidance, DOT, DHS, DOD, Congress, NTIA, and more. Full list here:
https://www.iamthecavalry.org/usgdisclosure

As for the implementation, the "devil is in the details" of how this section plays out. I would encourage a few things as this section gets discussion, debate, and alteration:

- The current 3 year DMCA exemptions for good faith research on things like Voting Machines, Cars, Medical Devices, and Consumer Electronics are already showing fruit and proving the value of making them permanent. These significant discussions and stakeholders would be instructive both for DMCA and for possible mirroring for CFAA.
- The Librarian of Congress and Copyright Office has recommended they would like these exemptions to be made permanent. Congress could consider giving that recommendation the strength of law. If I recall, the FTC has also suggested this. I am not a lawyer, but law professor Andrea Matwyshyn (also now a Non-Resident Senior Fellow for me at Atlantic Council) was directly involved in these exemptions and has specific analysis regarding the current S. 1691 wording.
- The Commerce NTIA Multi-Stakeholder Process for Coordinated Vulnerability Disclosure also yielded a template, two surveys, and guidance for the harder, multi-party disclosures – and these materials and Executive branch leaders will have valuable insight.
- While the bill does call out ISO 29147 which outlines a standard for receiving and responding to disclosures, it would be more complete to include ISO 30111 for the process of triage and resolution
- We would want to ensure the discovery and/or research itself was protected – and not merely hinge on the act of disclosure.

On Alternative Approaches to S. 1691 – and the Geo-Political Context:
Were another Mirai or devastating attack to occur and trigger a knee-jerk, domestic or international policy response, there are other methods that could stop the attacks, but many are quite dangerous and have less obvious downside/risks. They may be worth exploring, but in a vacuum, I fear some of the fastest and easiest fixes may play into the hands of our adversaries and oppressive regimes. For example:

- Nation Centric Internet Sovereignty/Filtering – Via the UN/ITU: Russia, China, and some of the Middle East and African nations have tried to advocate for Balkanization of the Internet – away from the current Multi-Stakeholder Internet Governance Model. This can enable greater censorship, surveillance, dissident tracking/oppression, etc.

- Enable Carriers to do Deep Packet Inspection and Filtering: This could get entangled with Net Neutrality debates and current safe harbor from the transmission of illicit/illegal material
- Destroy or “Brick” the devices: Many proposed this after Mirai – and things like BrickerBot actually did destroy some devices. This has serious risks, could cause property damage, and while people thought it was less of an issue for cheap IoT cameras, think of the harm to medical devices and industrial systems. Further, some vulnerable components like BusyBox found in cheap IoT – are ALSO found in these safety critical devices like medical equipment – so you may aim to destroy camera and end up affecting human life or capital equipment destruction.

Other countries have been hit hard too… like Germany by Mirai and the UK by WannaCry. It is my belief that if the US does not lead here, we will end up being affected by European policy changes – and/or those pushed by our enemies. I see this as a foot race to decide what we want – and harmonize with our international allies.

Time is the enemy. The time for hand waving and hesitation is over. We should measure twice, cut once – and seek a basis of evergreen and internationally effective policies, but the status quo will not stand beyond the next high consequence attack.

Reaching Critical Mass:
“I am The Cavalry” has published simple frameworks for primitives and table stakes on Connected IoT Devices:

A “5 Star Cybersafety Framework for Connected Vehicles” and a “Hippocratic Oath for Connected Medical Devices” (linked below). Both essentially say… All systems fail. Therefore, you need to be ready for failure across 5 dimensions. Essentially, the guidance asks manufacturers to tell the market how they:

1. Avoid Failure (Safety by Design)
2. Take Help Avoiding Failure (Third Party Collaboration – Vulnerability Disclosure Programs)
3. Notice & Learn from Failure (Evidence Capture)
4. Respond Quickly to Failure (Security Updates)

5. Contain & Isolate Failure (Segmentation & Isolation - of Critical Systems from Non-Critical Systems)

AUTO
https://www.iamthecavalry.org/domains/automotive/5star/

MEDICAL:
https://www.iamthecavalry.org/domains/medical/oath/

In government, throughout 2016 and 2017, several Executive & Legislative policies & documents have been converging around a few key themes surrounding minimum Cyber Hygiene – to better insulate us from harm caused by accidents and adversaries:

Below are a few examples:

- 2017 Executive Order on Cybersecurity:
  - “for too long accepted antiquated and difficult-to-defend IT”
  - “commensurate with the risk and magnitude of the harm”
  - “Known but unmitigated vulnerabilities are among the highest cybersecurity risks faced by executive departments and agencies"
  - “attacks that could reasonably result in catastrophic regional or national effects on public health or safety”
  - "cybersecurity risks facing the defense industrial base, including its supply chain"
  - https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal

- 2017 Congressional “Health Care Industry Cybersecurity Task Force”
  - Known Vulnerabilities Epidemic
  - Call for a required Software Bill of Materials or Medical Devices and Electronic Health Records Systems (EHR/EMR)
  - https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf

- 2016 Presidential Commission on Enhancing National Cybersecurity
  - “Nutrition Labels” for IoT to enable consumer choice
  - An exploration for the state of the law regarding Liability with regards to software and IoT
  - https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf

- 2016 US Commerce NTIA's Multi-Stakeholder Processes on:
  - Best Practices for Coordinated Vulnerability Disclosure
    - https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilities
  - Upgradability and Patching for Internet of Things

- 2016 DHS Strategic Principles for Securing the Internet of Things
  - Security by Design
  - Patch-ability
  - Software Bill of Materials
  - Coordinated Vulnerability Disclosure Programs
  - https://www.dhs.gov/news/2016/11/15/dhs-releases-strategic-principles-securing-internet-things

- 2016 FDA Post-Market Guidance (and prior 2014 Pre-Market)
  - Patching / Security Updates
  - Promotion of (and Incentives for) Coordinated Vulnerability Disclosure Programs

- 2016 FTC "Start with Security" 10 Principles
  - https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf