Operationalizing Sustainable Cybersecurity

What follows are prioritized but not exhaustive actions stakeholders across the internet ecosystem can take and work toward to build and sustain a more resilient network of networks, one that protects the security and privacy of the data driving the modern economy.

For product manufacturers:

- Following secure software development best practices, e.g., Software Assurance Marketplace; OWASP
- Publishing a software bill of materials that details the product development process
- Establishing a product's usage, lifespan, and end-of-life management
  - Using the Manufacturer Usage Description Specification
  - Updating purchasers when a product exceeds its supported life
  - Offering discounted upgrades to reduce population of insecure products
  - Ensuring where appropriate products fail safe to safe/secure mode
- Selling products that are secure by design with no known defects
- Developing vulnerability management and patch dissemination policies and processes, including automatic updates where appropriate
- Participating in information sharing and analysis organizations
- Educating workforce about cybersecurity, including application outside the work environment

For enterprise network operators:

- Utilizing the NIST Cybersecurity Framework – identify, protect, detect, respond, recover
  - including the supporting policies and procedures, e.g., incident response plan
- Requiring a software bill of materials for purchases of internet-connected devices
- Validating the integrity of hardware and software
- Developing patch management processes to ensure products remain up to date
- Maintaining least privilege across the network
- Securing access to infrastructure devices
- Segregating networks and functions
- Using Domain Message Authentication Reporting and Conformance (DMARC)
- Implementing Best Common Practice 38 & 84 - ingress and egress filtering
- Participating in information sharing and analysis organizations
- Educating workforce about cybersecurity, including application outside the work environment

For civil society and consumers:

- Educating themselves about cybersecurity
- Practicing good cyber hygiene
    - Backing up data
    - Installing updates when informed by manufacturers
    - Using strong passwords and not reusing them
    - Using two-factor authentication
    - Reducing opportunities to be a victim of social engineering
    - Using web browsers that filter bad domains
- Reinforcing good hygiene with friends and family
- Investing in products with robust security, as evidenced by, for example, the Digital Standard
- Holding accountable organizations that fail to adequately develop and secure products by using their competitors, where available

For governments:

- Leading by example in procurement, enterprise operations, personnel and national education, and research and development
- Convening stakeholders to build cybersecurity capacity internationally
- Supporting and participating in international standards organizations
- Improving incentives for stakeholders to implement sustainable cybersecurity, including by reevaluating liability frameworks
- Collaborating to investigate and whenever possible prosecute criminal misuse of ICTs
- Refraining from activities that undermine public trust in ICTs

Next steps

We propose to facilitate and participate in a series of multistakeholder conversations about this paper and the actions it outlines. Agenda items for these conversations include:

- Are these the right actions for these actors? What's missing?
- What are the legal and/or policy challenges limiting these actions' implementation?
- What incentives could spur broader adoption of these actions?
- Which actions would make useful case studies?

This list originates from a policy white paper entitled "Securing the Modern Economy: Transforming Cybersecurity Through Sustainability," by Megan Stifel, Cybersecurity Policy Director. You can read the paper at publicknowledge.org/SustainableCybersecurity.