Opening Statement of Chairman Robert E. Latta
Subcommittee on Communications and Technology
"Cybersecurity"
January 11, 2024

Good morning, and welcome to the Communications and Technology subcommittee's first hearing of 2024!

The telecommunications industry stands as the backbone of our interconnected world, facilitating seamless communication and driving the digital economy. But with increased connectivity comes a growing threat landscape that demands vigilant cybersecurity measures to defend against malicious actors and ensure the resilience of our telecommunications infrastructure.

Astonishingly, every 39 seconds a cyberattack occurs, underscoring the relentless nature of the challenges we face in safeguarding our digital infrastructure.

Industry faces evolving cyber threats, ranging from general, brute force attacks to sophisticated and targeted deception. Common threats include Distributed Denial of Service attacks, which disrupt service availability by overwhelming networks with traffic; phishing attacks targeting users to compromise sensitive information; and ransomware attacks, which paralyze operations and hold critical data, like patient health information, captive.

Additionally, the rise of Internet of Things (IoT) devices allow us to be more connected to our surroundings than ever before. From smart home applications to wearable gadgets, IoT devices have transformed the way we live and work. However, their proliferation creates new and complex cybersecurity challenges that need careful consideration and robust solutions. With billions of interconnected devices, each with its own set of vulnerabilities, the possibility of attacks expands exponentially.

To combat these threats, the Federal Communications Commission (FCC) announced the creation of a voluntary cybersecurity labeling program for smart IoT devices with the goal of protecting American users. This program, called the U.S. Cyber Trust Mark, would place a logo on products that meet a basic level of security. The security requirements would be developed by the FCC and based heavily on the work of the National Institute of Standards and Technology (NIST).

While I still have a few key questions regarding the "*voluntary*" nature of this program, particularly in light of the FCC's recent net neutrality and digital discrimination orders, I am pleased that the Commission is taking proactive steps to protect Americans from cyberattacks.

As we navigate the complex landscape of cybersecurity, collaboration between industry stakeholders, government agencies, and the cybersecurity community is paramount. Developing and sharing best practices, threat intelligence, and technological innovations will strengthen our collective defenses against evolving cyber threats.

The integration of Artificial Intelligence (AI) has emerged as a sharp, double-edged sword in the security landscape. It acts as both a crucial tool in the defense against cyber threats and as a potent enemy. AI technologies, such as machine learning algorithms, play a pivotal role in augmenting cybersecurity capabilities. AI enables rapid analysis of vast datasets to identify potential threats, enhance detection, and automate response mechanisms. AI-driven threat intelligence allows for proactive identification and mitigation of emerging risks.

Artificial Intelligence has also been weaponized to extend offensive capabilities, as threat actors increasingly leverage the technology to conduct more sophisticated and targeted attacks. Adversarial machine learning, where attackers manipulate AI algorithms, presents a new challenge that requires continuous innovation in defensive strategies.

At today's hearing, we will also hear from experts on Border Gateway Protocol security. This postal service for the Internet ensures that your information gets to its intended destination in as few steps as possible. While Internet routing security might not be the most attractive topic for a congressional hearing, it is our job to discuss these security issues and protect the American people.

Thank you to our witnesses, and I look forward to the discussion.