MEET the THREAT

States Confront the Cyber Challenge

Q&A: Internet-of-Things

What is the Internet-of-Things?

The Internet-of-Things (IoT) describes how commercial industries are including Internet connectivity in a wide range of electronic devices that are traditionally thought of us "dumb," such as door locks, light bulbs, or surveillance cameras. Integrating these devices and others into the global Internet means that security cameras can stream video feeds to smartphones; utilities can manage the electric grid by gathering data from smart meters; and hospitals can monitor patients remotely. IoT devices are a key component of "smart cities," and they will play an important role in future "smart state" projects.

Why is the IoT a security risk?

Virtually all electronic devices that connect to the Internet—whether they are desktop PCs, smartphones, or IoT devices—pose security risks. Cyber criminals can infiltrate vulnerable systems to hijack them or steal data. In November 2016, criminals assembled hundreds of thousands of IoT surveillance cameras and digital video recorders into a "botnet" that shut down key Internet infrastructure. A much smaller botnet succeeded in disabling 9-1-1 call centers in at least a dozen states. Different dangers entirely arise from connected devices that interact with the physical world, such as gas generators or heart monitors, which hackers can sabotage to inflict physical damage.

Why is IoT security treated differently from other cybersecurity issues?

What distinguishes those devices known as "IoT" from normal computers are security standards. Most PCs and mobile devices come packaged with cybersecurity automatically. By contrast, many IoT devices do not include any meaningful security measures because their electronic brains are too simple. Other IoT gadgets do have security measures, but cannot be regularly updated to adapt to new cyber threats. In addition, the explosive growth in IoT devices—expected to number in the tens of billions in the next five years—greatly complicates the job of security professionals by expanding the number of assets they need to protect while simultaneously growing the number of weak points that hackers can exploit.

What should governors do about the IoT?

The further deployment of the IoT is inevitable, and states should prepare to manage the associated risks to government services and the economy. Governors can begin to mitigate these risks by:

- **Isolating IoT networks**: From the earliest stages of technology projects, isolate insecure IoT networks from core business functions in accordance with risk management principles.

- **Procuring securely**: Requests for proposals and contracts involving technology should include cybersecurity commitments based on industry best practices.

- **Auditing IoT devices**: Maintain and regularly update a comprehensive inventory of all Internet-connected devices owned, operated, and licensed by state authorities or connected to state networks. Coordinate with localities to do the same for municipal networks.

- **Clarifying authority**: Issue formal policy assigning responsibility for securing publicly-owned IoT devices and the data generated by them.