OutSecure Inc

OUTSECURE

CYBERSECURITY STRATEGY CREATION COMPANY

Digital Security. Simplified.

www.outsecure.com

2 TRAP FALLS RD SUITE 401 SHELTON CT
www.outsecure.com (203)816-8061

Today's Topic

Data Unlimited: Using Analytics and Integration to Put City Data to Work

Cities regularly grapple with how to collect, analyze, integrate and then use the data collected from ubiquitous data collection sources. Join experts on data integration to learn about creating a data strategy for your city. Learn about what questions to ask and how to set priorities. Bring your experiences and challenges to share.

About me..

- Security thought leader, Founder Member of IoT Security Foundation, a industry consortium of global IoT leaders, member EC-Council IoT board, Cybersecurity & Privacy advisory council NIST Global Cities Technology Council.
- Technical cyber expert Subject Matter Expert (SME) & Mentor for Cybersecurity.
- 22 years working for Global Fortune 500 Companies creating strategic risk based programs to help business's survive and be profitable.
- Writing a book on Cyberwar: A business impact perspective.
- Guest commentator and writer for local television, print and online media. Featured on, among others, Forbes, Huffington Post and *various industry organizations publications.*
- President of OutSecure, A cybersecurity security company helping clients stay profitable and anticipate cybersecurity risks to their business.
- Chair & Founder Northeast Annual Cybersecurity Summit, NEACS – a security summit for business leaders. - *Summit – Premier Security, Governance & Audit event for Business leaders;*
- President CT Chapter of ISC2, helping spread security awareness in the security community.

The Irony of Big Data and IoT

Big data from small devices.

5 quintillion bytes of data *produced every day.*

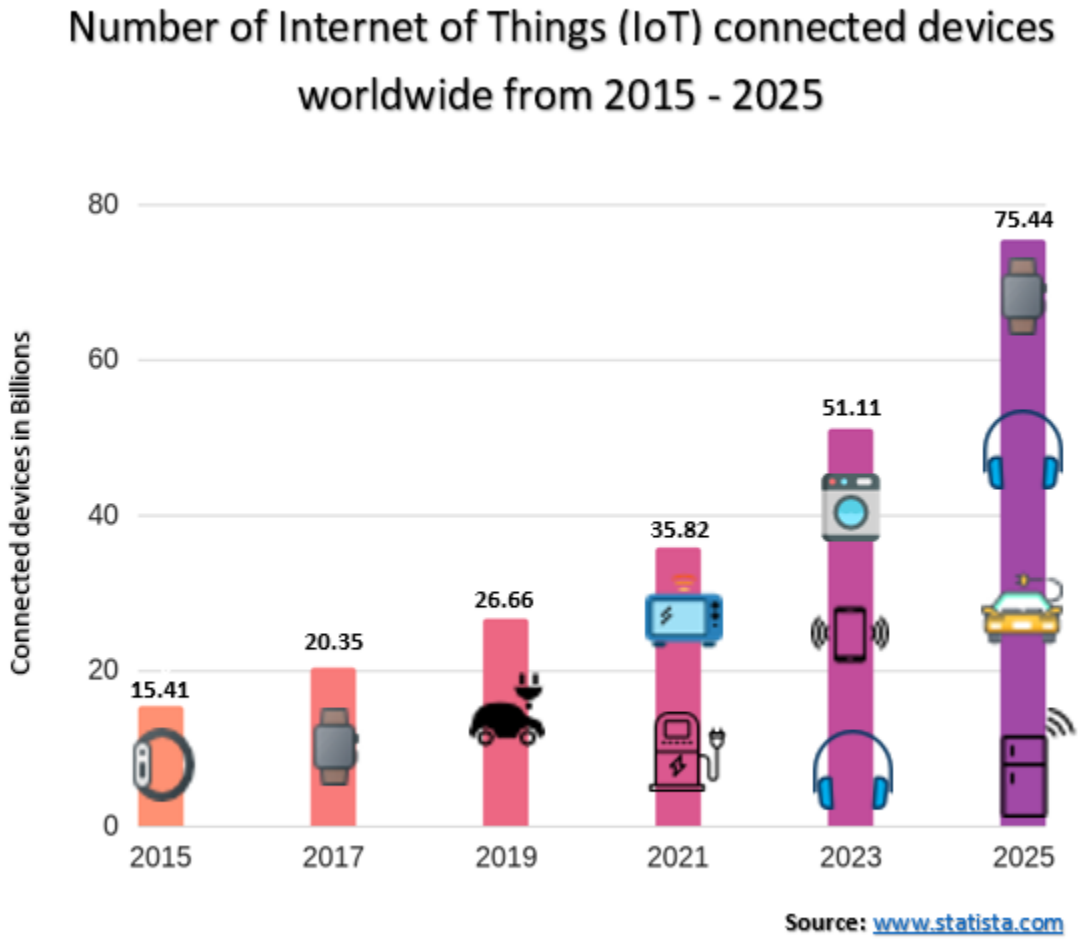
A quintillion is

Million 1,000,000 (6 zeros)
Billion 1,000,000,000 (9 zeros)
Trillion 1,000,000,000,000 (12 zeros)
Quadrillion 1,000,000,000,000,000 (15 zeros)
Quintillion 1,000,000,000,000,000,000 (18 zeros)

Harvard Business Review found that:

- ***Less than half*** *of structured data is actively used in decision making*
- ***Less than 1%*** *of unstructured data is analyzed or used at all*

Human population is 7.9 Billion



We need a strategy for IoT Success

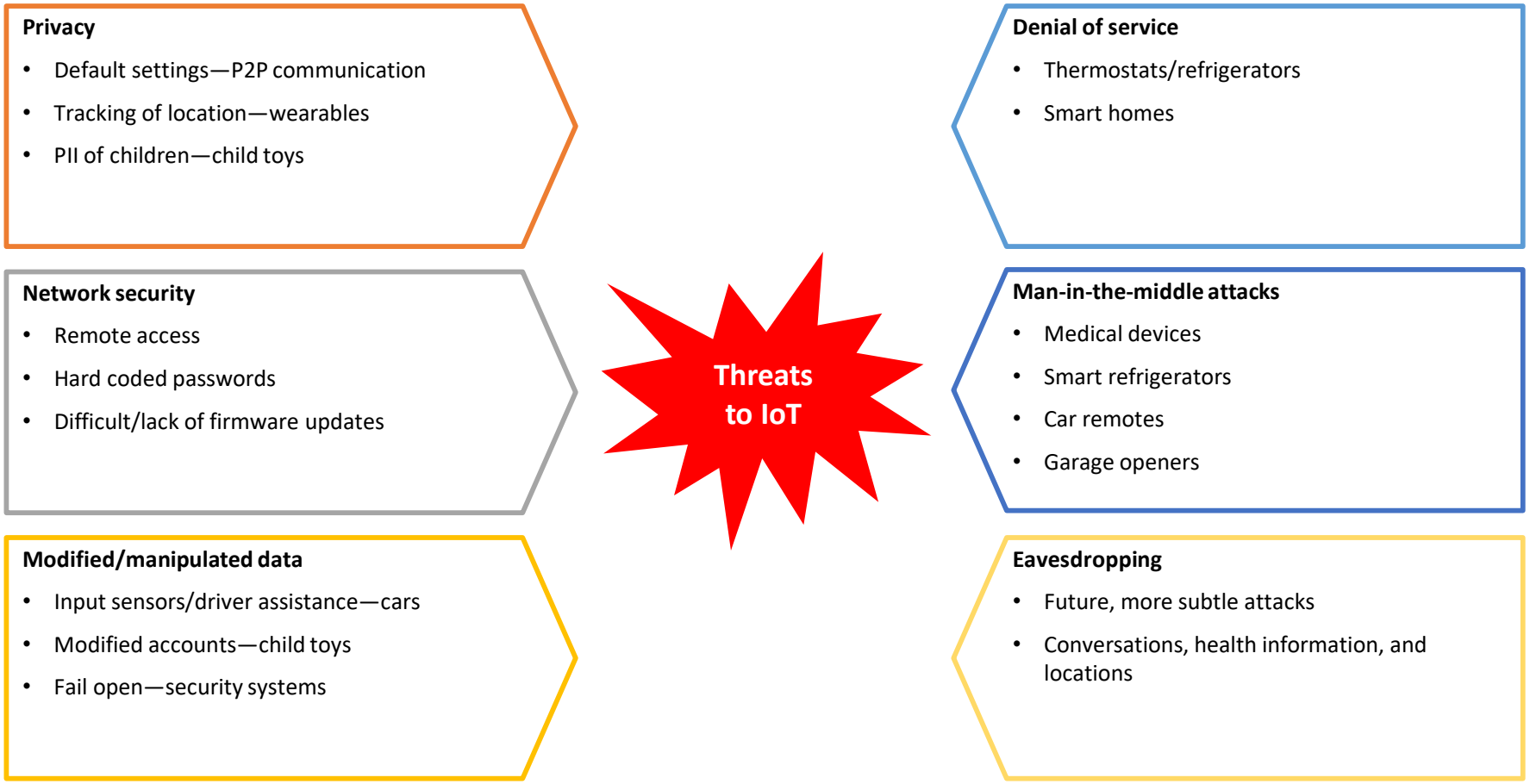
1. What is the desired outcome;
2. Create value of data from various sources;

3. Data Analytics - analyzes IoT data to solve problems or create new opportunities. Companies can create competitive advantage with IoT technology by owning the data or algorithm that defines a beneficial outcome. Today, very little of the data generated by Internet-connected things are actually used, and those data that are used are not fully exploited. The oil and gas industry, for example, which has as many as 30,000 sensors on a single offshore oil rig, is using less than one percent of the information gathered from those devices for decision making, according to McKinsey. And most of the data that are used—for example, in manufacturing automation systems on factory floors—are utilized only for real-time control or anomaly detection.

4. Start small and scale up…

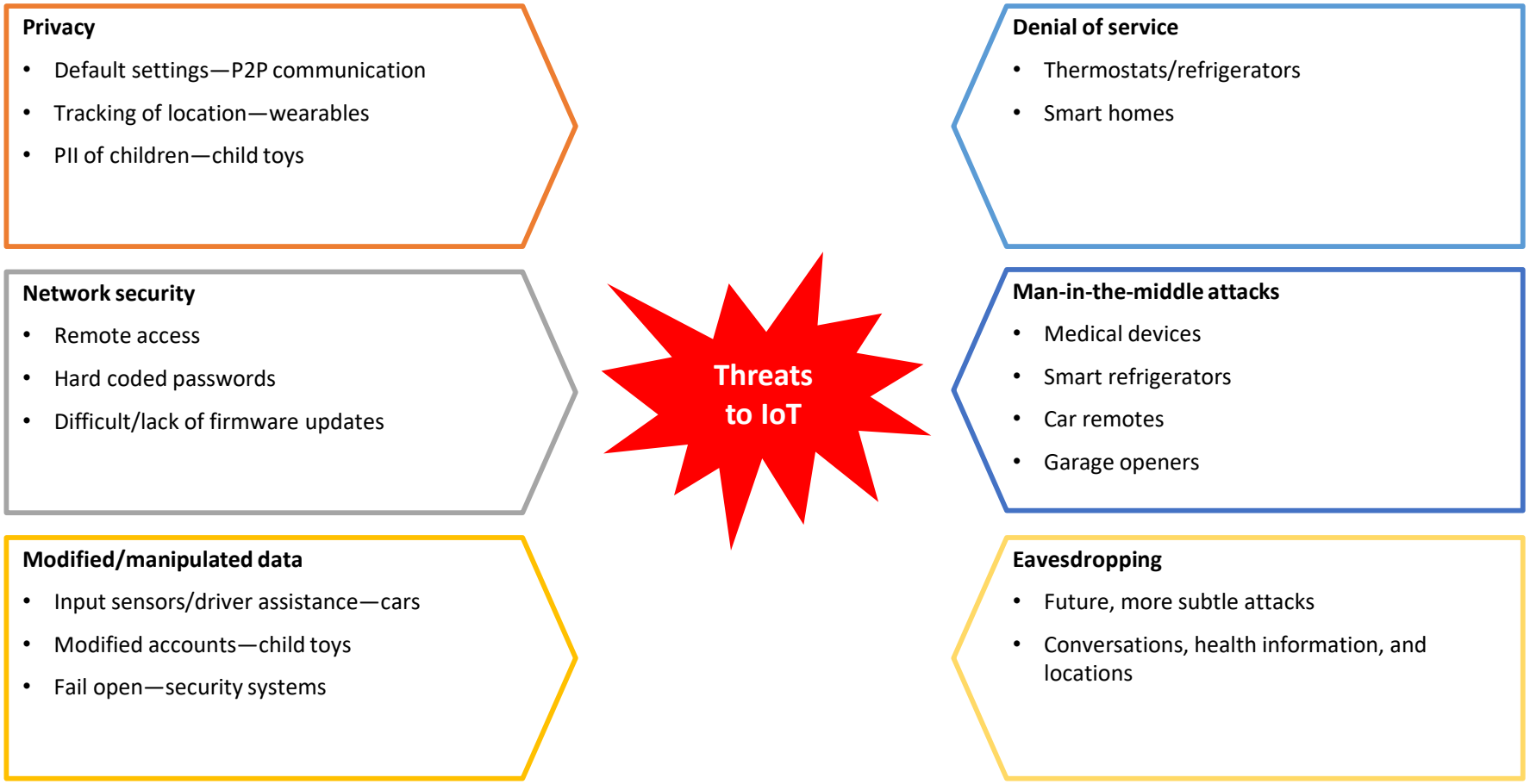
Threats resulting from IoT devices

The large amount of data collected, transferred, and stored by IoT devices, increases surface area for attackers to target and exploit vulnerabilities



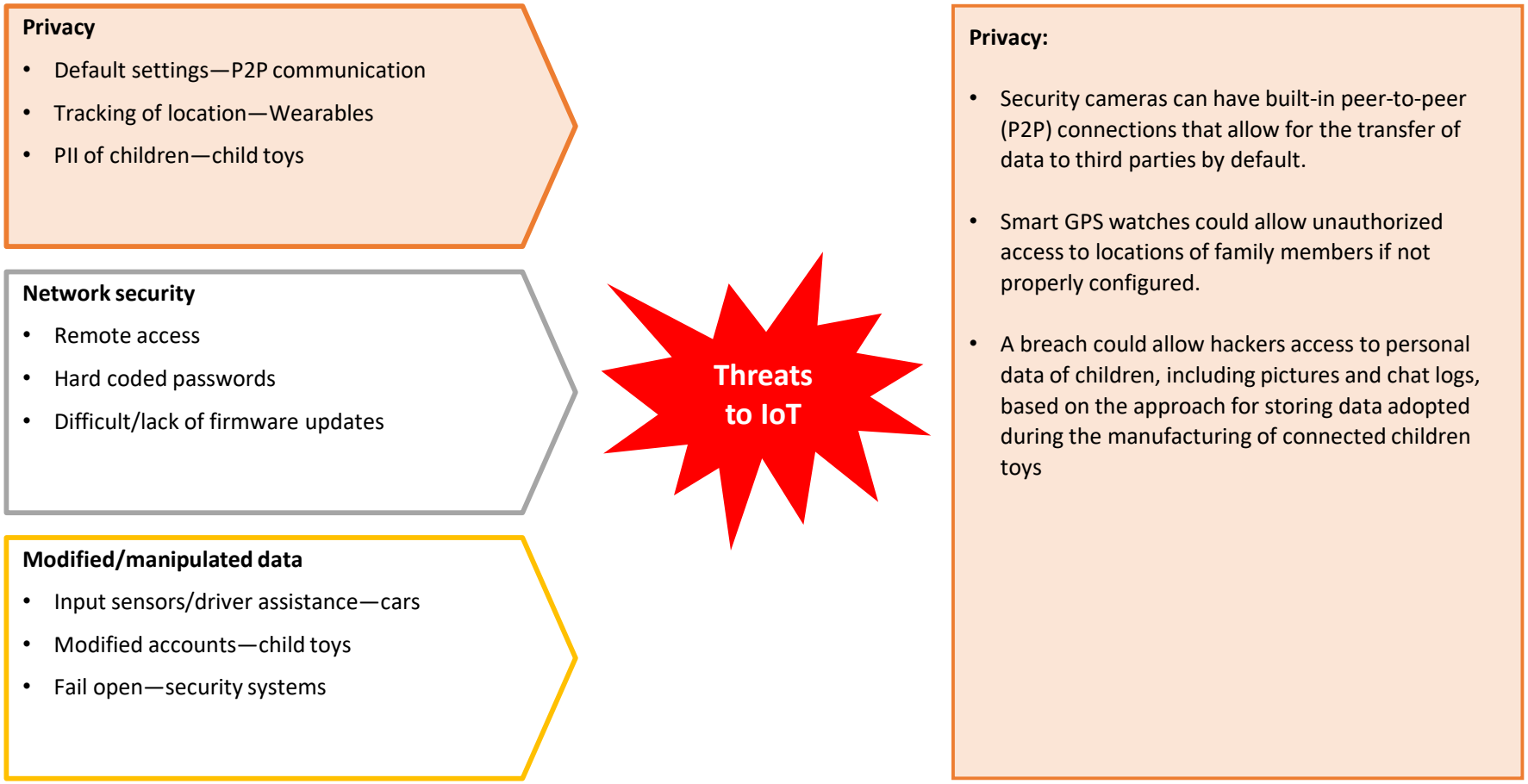
Threats resulting from IoT devices

The large amount of data collected, transferred, and stored by IoT devices, has opened the door for attackers to target and exploit vulnerabilities



Threats resulting from IoT devices (cont.)

Privacy



Threats resulting from IoT devices (cont.)

Network security

Privacy

- Default settings—P2P communication
- Tracking of location—Wearables
- PII of children—child toys

Network security

- Remote access
- Hard coded passwords
- Difficult/lack of firmware updates

Modified/manipulated data

- Input sensors/driver assistance—cars
- Modified accounts—child toys
- Fail open—security systems

Network security:

- Vulnerabilities have been discovered in household connected devices, allowing hackers to gain remote access and use those connections as a jumping point to the rest of the network
- Many devices contain hardcoded passwords that allow accounts to be accessed remotely
- Some manufacturers do not use up-to-date patches, and cannot push updates to consumers when vulnerabilities are identified
- Many manufacturers do not inform consumers that firmware updates may be needed for their products and consumers are unable to easily update firmware

Threats resulting from IoT devices (cont.)

Data security/integrity

Privacy

- Default settings—P2P communication
- Tracking of location—Wearables
- PII of children—child toys breach

Network security

- Remote access
- Hard coded passwords
- Difficult/lack of firmware updates

Modified/manipulated data

- Input sensors/driver assistance—cars
- Modified accounts—child toys
- Fail open—security systems

Modified/manipulated data:

- Manipulation of car input sensors could result in injuries or hazards to passengers
- Hackers could potentially hijack car components including the breaking system by hacking the car's driver assistance system and onboard computer
- Connected toys could allow attackers the ability to gain unauthorized access to account profiles including stored information such as toy configurations and child interaction details
- Security systems could be manipulated to return incorrect data including reporting that doors/windows are closed, while in fact they are open. This could result in a failure to identify actual alarm events

Threats resulting from IoT devices (cont.)

Denial of service attacks

Denial of service (DoS):

- IoT devices often have minimal computing powers, which makes it difficult to process many requests at the same time
- Thermostats or refrigerators could be susceptible to Denial of Service attacks that would not allow the products to properly manage temperatures
- Alternatively, a thermostat could be hijacked to send spam alerts or emails at an incredibly high rate
- DoS attacks against smart homes, homes with HVAC, lighting, garages, and other IoT connected devices, could render the homes temporarily inoperable

Denial of service

- Thermostats/refrigerators
- Smart homes

Man-in-the-middle attacks

- Medical devices
- Smart refrigerators
- Car remotes
- Garage openers

Eavesdropping

- Future, more subtle attacks
- Conversations, health information, and locations

Threats resulting from IoT devices (cont.)

Man-in-the-middle attacks

Man-in-the-middle attacks:

- Many medical devices have been identified as being susceptible to attacks when connected for the purpose of 1) monitoring or 2) providing human responses for the device to execute
- Smart home devices using e-mail credentials for communication could allow an attacker to gain unauthorized access to those e-mail credentials if security is properly configured
- Although not typically IoT devices, car keyless entry remote signals could be spoofed, allowing for a anyone to use a $30 device to enter a car later
- If a garage opener, with a feature to disable a security system, is compromised, an attacker could have access to the entire home

Denial of service

- Thermostats/refrigerators
- Smart homes

Man-in-the-middle attacks

- Medical devices
- Smart refrigerators
- Car remotes
- Garage openers

Eavesdropping

- Future, more subtle attacks
- Conversations, health information, and locations

Threats resulting from IoT devices (cont.)

Eavesdropping

Eavesdropping:

- Similar to the previous topics of privacy, network security and man-in-the-middle attacks, eavesdropping on IoT devices can expose consumers to future threats
- Malicious attackers can use data eavesdropped / collected from IoT devices or networks to plan or perform more subtle attacks that appear to be normal user actions (e.g., disabling an alarm system, performing commands using the user's credentials)
- Unsecure / unencrypted data being transferred from IoT devices can expose conversations, health information or locations, as well

Denial of service

- Thermostats/refrigerators
- Smart homes

Man-in-the-middle attacks

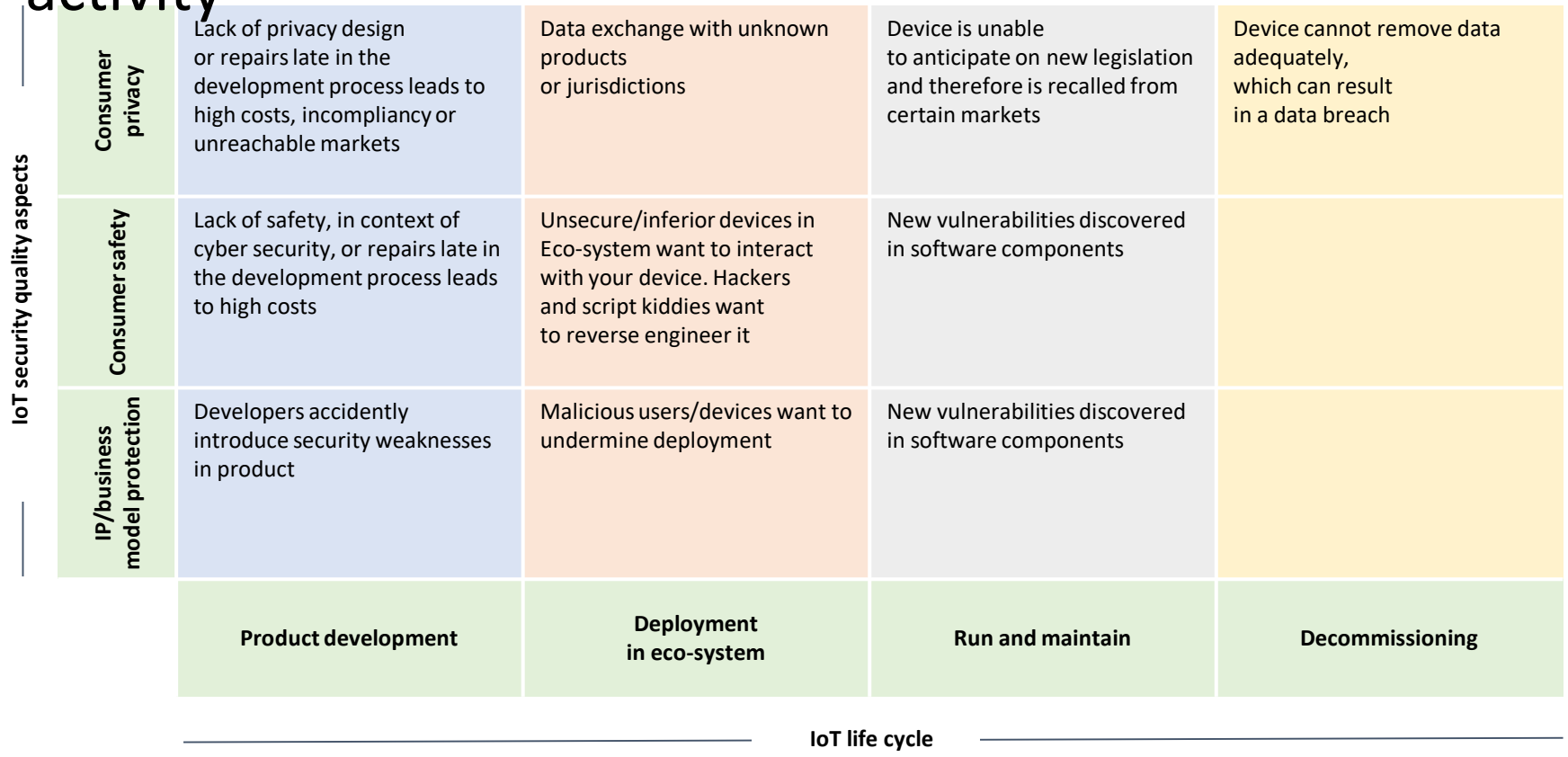
- Medical devices
- Smart refrigerators
- Car remotes
- Garage openers

Eavesdropping

- Future, more subtle attacks
- Conversations, health information, and locations

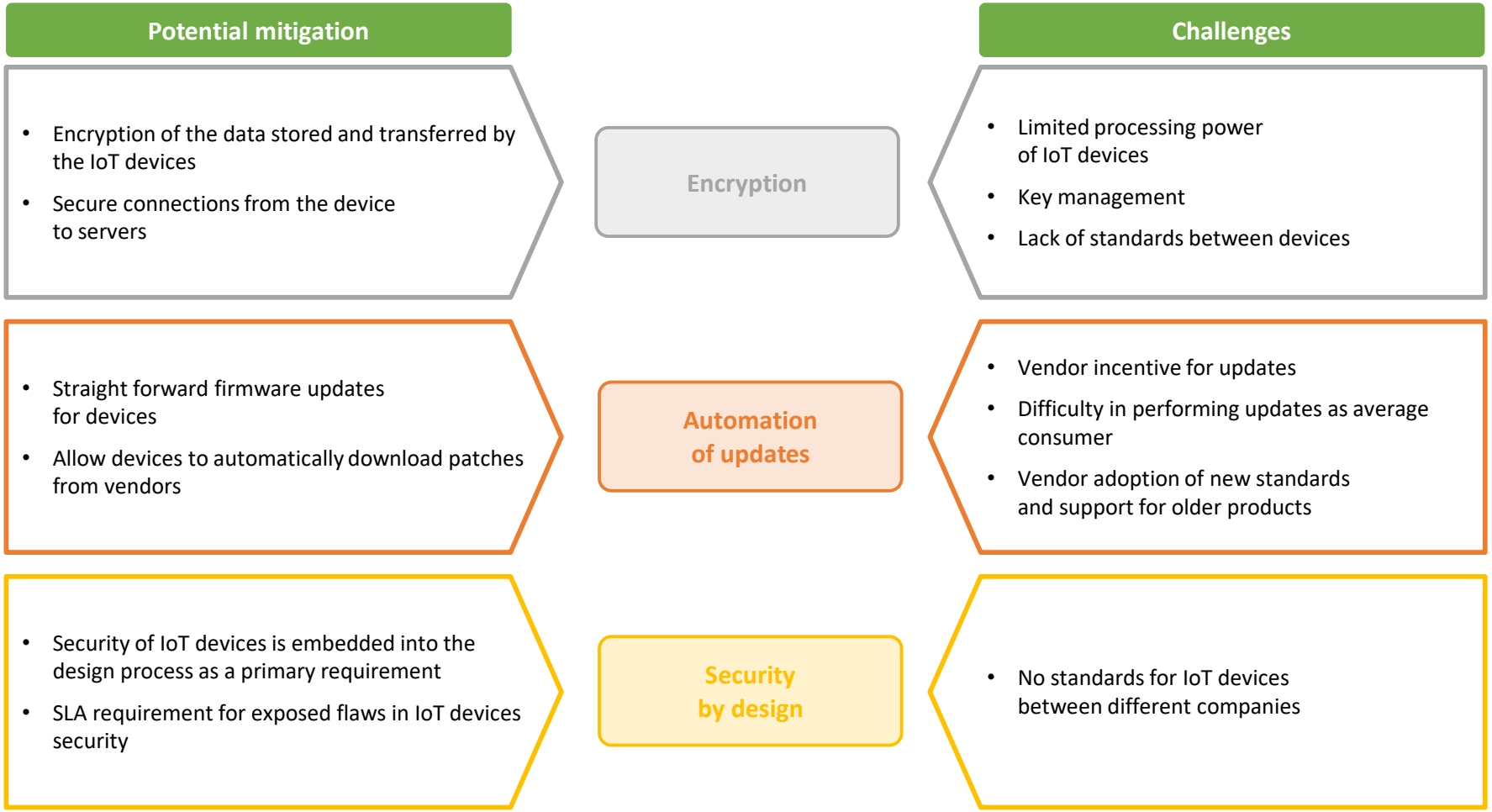
IoT security risk throughout the lifecycle

- IoT security must not be a one-time, “check the box” activity



Mitigations to IoT threats

Although many mitigations/solutions may appear to be straightforward, the limited processing power of many IoT devices presents challenges to manufacturers



Contact Information

We help our clients in solving complex security challenges:

- **Creating Risk Based Security Roadmaps**
- **Identifying Risks and Solutions for Existing and Emerging Technology**
- **Managing Third Party Risks through our Platform**

Office: 203.816.8061
Email: pamela.gupta@outsecure.com

OutSecure Headquarters:
Shelton Pointe, Suite 401
2 Trap Falls Road
Shelton, CT 06484-4665
http://www.outsecure.com