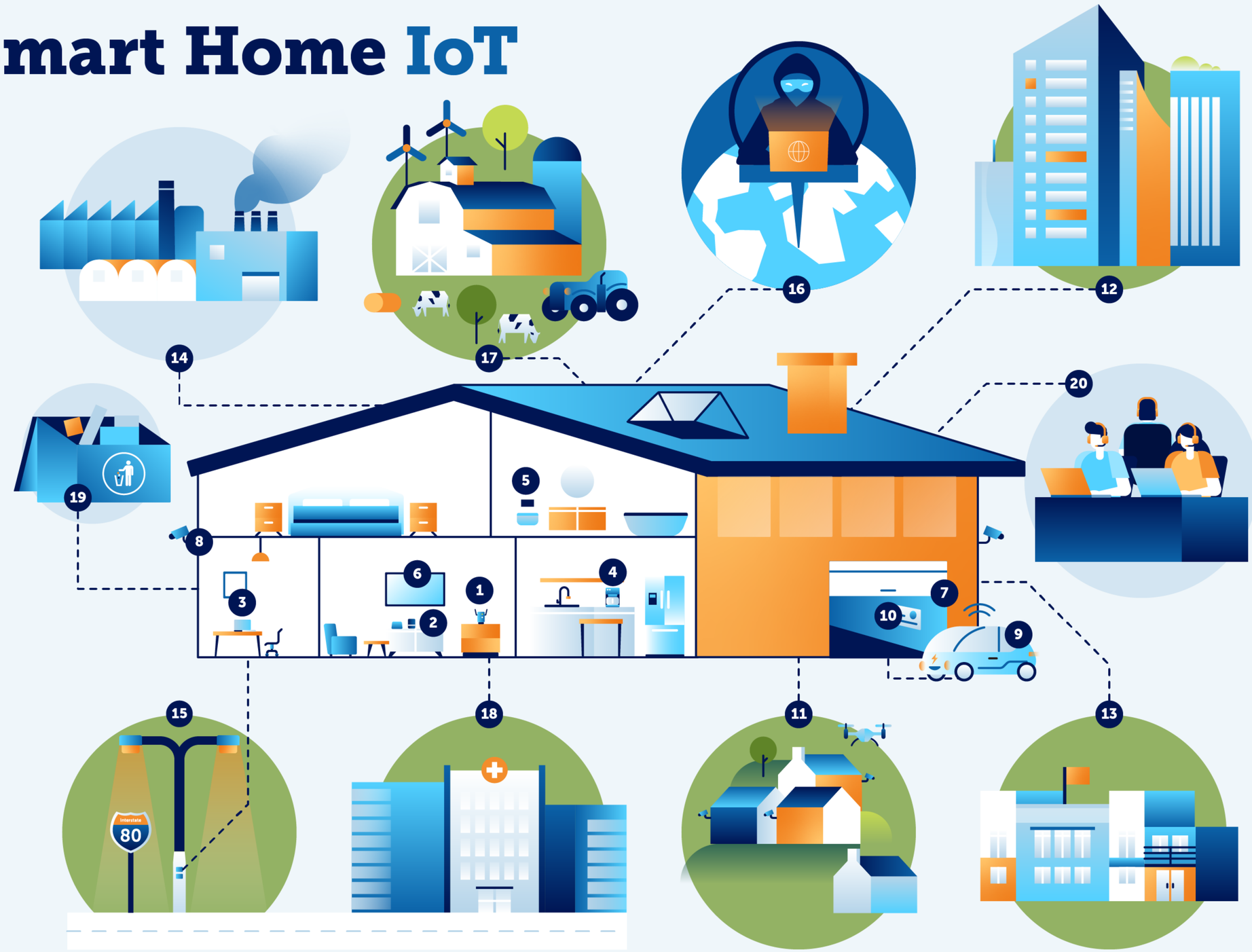
PSB Smart Home IoT

OCTOBER 2021

1. **Home Wi-Fi routers & networks**
2. **Smart home controllers & hubs**
3. **Computers**
   (e.g., laptops, desktops, smart phones)
4. **Smart appliances**
   (e.g., coffee makers, refrigerators)
5. **Smart plumbing**
   (e.g., smart toilets, water savers)
6. **Smart entertainment**
   (e.g., smart TVs, personal digital assistants)
7. **Smart entries to homes**
   (e.g., garage doors, windows, front doors)
8. **Smart security cameras**
9. **Smart vehicles**
   (e.g., cars, semi-trucks, trains)
10. **Smart utilities meters**
11. **Nearby smart devices**
    (e.g., neighbors' security cameras, drones)
12. **Business buildings with IoT tech**
    (e.g., surveillance, temperature controls)
13. **School buildings with smart tech**
    (e.g., student trackers, security systems)
14. **Factories with smart technologies**
    (e.g., AI-controlled robots)
15. **Smart roads, rail & waterways**
    (e.g., smart light poles, traffic controllers)
16. **Worldwide hackers**
    (e.g., nation-state, cybercriminals)
17. **Farms with smart tech**
    (e.g., self-driving tractors, livestock tags)
18. **Healthcare providers**
    (e.g., smart medical devices, smart pills)
19. **IoT tech disposal**
    (e.g., put in trash, sold to others)
20. **Call center**
    (e.g., customer service, help desk)



Risks

The wide range of smart devices used within smart homes reach far beyond the boundaries of the home. Indeed, they can connect and communicate with other devices, systems and individuals throughout the globe. This creates a world of risks within your own comparatively small smart home. Here are a few of the risks, which represent real-world incidents that have occurred utilizing smart devices (see the IoT risks descriptions at https://privacysecuritybrainiacs.com/resources/infographics/IoT/):

- ✕ Unauthorized access to networks
- ✕ Unauthorized digital access to devices
- ✕ Unauthorized access to data repositories
- ✕ Human factors
- ✕ Physical security and safety
- ✕ Privacy harms
- ✕ Violated laws & regulations

Security Must-Haves

To safeguard against the listed risks, smart devices should be secured by using the following as appropriate to the use and purpose for each smart device (see the IoT safeguards descriptions at https://privacysecuritybrainiacs.com/resources/infographics/IoT/):

- ✓ Network security
- ✓ Device security
- ✓ Data security
- ✓ Encryption
- ✓ Strong authentication
- ✓ Device maintenance & updates
- ✓ Physical security
- ✓ Human awareness
- ✓ IoT product support services
- ✓ Customer control of their own data

© Privacy & Security Brainaics. All Rights Reserved.