CYBALT

The New Challenges For IoT Data Privacy And Data Integrity

Cybalt Inc. Suite #510, 2701,
North Dallas Parkway, Plano, TX

discover@cybalt.com

The New Challenges for IoT Data Privacy and Data Integrity

Companies have historically managed assets such as property, plants, equipment, inventory, cash, and intellectual property. In today's digital world, a new type of asset is emerging – data. Data, specifically the Internet of Things (IoT) data, has become a strategic asset that can be sold and exchanged. Due to the rise in data availability and data-driven insights, more and more data is being exchanged within and among companies. This has spawned a new data economy built upon using data to generate value through both internal and external means. The Monetization of this IoT data is what is called *The Data Economy*.

The Internet of Things (IoT) will reach an eye-opening 46 billion devices by the end of 2022. By 2030, this figure is expected to jump to 125 billion. With the introduction of IoT products, everything from smart thermostats to fitness trackers, the privacy and security of such features become suspect. Because of the huge risks of data exposure, your PII being generated by IoT, and the data economy monetizing it and sharing it, more than 31 states in the U.S.A. are developing and adopting new privacy laws.

The Definition of Personal Information Has Changed

The new U.S. privacy laws are changing how the industry defines personal information. The new types of personal information now considered in need of protection include:

- Biometric information.
- Physiological data.
- Biological and chemical characteristics.
- Behavioral patterns.
- DNA (single or in combination with other identifying data to establish an individual's identity).
- Iris imagery, retina, fingerprinting, face, hand, palm, vein patterns, voice recordings, keystroke patterns or rhythms, gait patterns, sleep, health, or exercise data.

The push for better privacy protections is being driven by the need to protect these new forms of privacy data created by IoT and the digital economy monetizing the sharing of it between parties. While some organizations have a robust grasp of *privacy risk management*, a common understanding of many aspects of the topic is still not widespread. In response to the organizational privacy risk management dilemma, in December 2020, NIST released its new *Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0.*

Since its release in 2014, the NIST Cybersecurity Framework has helped organizations to communicate and manage cybersecurity risk. But according to NIST, while managing cybersecurity risk contributes to managing privacy risk, it is not sufficient, as privacy risks can also arise by means unrelated to cybersecurity incidents.

The new NIST Privacy Framework is to consider *privacy events* and describes *data actions* and *data processing* collectively, through a complete life cycle from data collection through disposal. This data action lifecycle includes the collection, retention, logging, generation, transformation, disclosure, sharing, transmission, and disposal of data. And according to the Privacy Framework, *Data Processing* is the collective set of data actions.

The NIST Privacy Framework has five core functions including *Identify-P, Govern-P, Control-P, Communicate-P, and Protect-P.* These core functions specific to privacy denoted by the "-P", can be used in conjunction with the Cybersecurity Framework Functions to manage all aspects of privacy and cybersecurity risks. But it is the *Control-P* and the *Protect-P* functions that are proving to be unusually difficult for organizations.

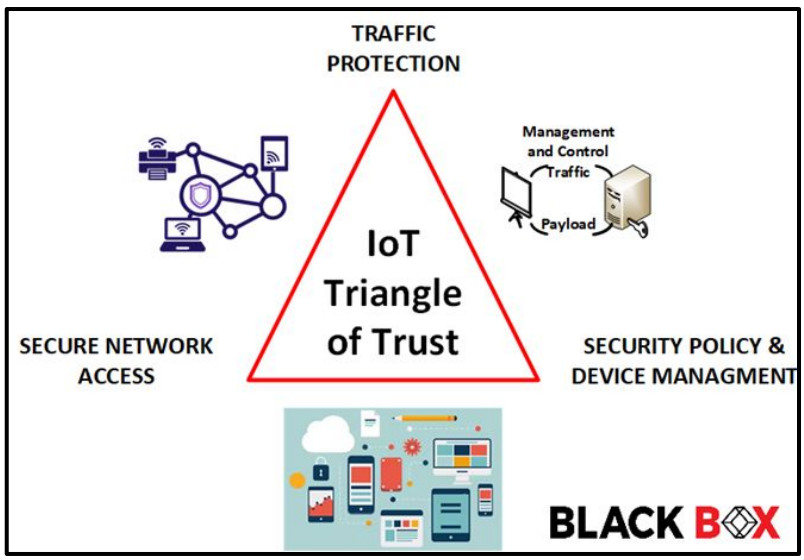
IoT Inventory and Mapping

The first category of controls in the NIST Privacy Framework, Inventory and Mapping, is appearing to be one of the biggest challenges to organizations as they expand their IoT environment. Many organizations are finding maintaining a simple inventory of their IoT a daunting task as each business unit wants to deploy their version of IoT in their way. Sometimes these deployments are overseen by the IT and Information Security Departments, oftentimes they're not. And mapping is proving equally challenging for hospitals for example, because each of their medical IoT devices ultimately, connects to the Electronic Health Records system and thus, within HIPAA scope.

Data Mapping is illustrating the data actions and associated data elements for systems, products, and services and their interactions with owners, operators, third parties, and their systems. Documenting and visualizing these interactions is a huge task on its own, especially at the speed organizations are growing their IoT footprint and incorporating new IoT features.

The IoT Triangle of Trust

Using the hospital again in the example, different departments are wanting to deploy IoT medical devices for their healthcare reasons. The lab wants IP-enabled centrifuges and microscopes, the ER wants IP enabled gel warmers and syringe pumps, and the surgical wards want IoT patient lifts and electrosurgical devices. But oftentimes, these departments make decisions based upon what's easiest to adopt with their legacy systems or what's supported by the EHR system, NOT by what adheres to corporate IT and information security policy.



This leads us to the IoT Security Triangle of Trust. The IoT Triangle of Trust identifies that every device must comply first, with the organization's security and device management policy. These security and device management policies address the "what" data privacy information needs to be protected when the IoT device is added to the network and the "how" data privacy protections will be protected. The IoT Triangle of Trust ensures that the following information security protections are in place:

1. **Security and Device Management Policy**

- Does the device comply with the organization's software standards?
- Does the device support logging and reporting features?
- Does the device support encryption for data in use and at rest?
- How is vulnerability management addressed?

2. **Secure Network Access**

- Is the device sanctioned and approved to be on the network?
- How are secure network authentication and authorization granted and enforced?
- What visibility can be achieved – where is the device now and where has it been?
- How is security posture identified and enforced? The IoT device needs to be at a certain software and patch level or it will not be allowed on the network according to policy.

3. **Traffic Protection**

- Traffic must be encrypted in motion and at rest.
- Is traffic that leaves the IoT network scanned for viruses and malware before crossing network boundaries and before reaching the EHR database?
- Are the traffic risks of IoT Cloud fully addressed?
- You can't control what you can't see. Is IoT traffic, especially traffic considered to contain PII, monitored and viewed?

The huge onslaught of IoT devices and its new data economy has forced states in the U.S. to adopt new privacy laws. These changes include how we define personally identifiable information and how we must use new standards like the NIST Privacy Framework to Identify, Govern, Control, Communicate, and Protect privacy data. IoT risk management has led to the development and application of privacy protections across the entire data life cycle including privacy data action and privacy data processing.

The Privacy Framework and the IoT Security Triangle help organizations answer fundamental questions like, "What are the impacts to individuals as we develop our systems, products, and services?" And "Are we accounting for the unique needs of the organization while ensuring IT security and privacy standards are adopted and enforced?