The Internet of Things (IoT) is one of the fastest growing technologies today due to its wide potential of applications. However, it also comes with security concerns like cyber attacks and software vulnerabilities, which makes customers hesitant in using IoT devices. This is especially true for organizations that deal in sensitive data such as healthcare, [retail](http://www.cardzgroup.com/ScratchCard.html), manufacturing, finance, and logistics industries.

So, what is IoT? Simply put, it is a network of connected smart devices that can exchange data via internet without requiring any human involvement. The technology finds its applications in a number of industries including logistics, agriculture, healthcare, automotive, and more. Depending upon the requirements, smart devices can range from a simple sensor to high-level DNA analysis hardware.

**What is IoT Privacy and Security?**

IoT security involves a set of practices and approaches that protect all the devices, processes, networks, and technologies from a wide range of cyber threats. IoT security matters because organizations with IoT applications need to be extra vigilant about system security and critical customer data. A small vulnerability can result in a cyber attack or system failure, which can directly affect hundreds of people. For instance, traffic lights that stop working suddenly can result in road accidents. Moreover, it is important to protect Personally Identifiable Information (PII) of customers, which is a requirement that must be fulfilled according to cybersecurity standards and regulations. Failure to protect it can result in loss of customer trust and eventually reputational damage to the organization.

**Common IoT Privacy and Security Challenges**

Maintaining security of IoT systems is a challenging task and it is important to have awareness of potential risks and challenges. Here are some common privacy and security challenges with the Internet of Things.

1. **Software Vulnerabilities**

Many smart devices have limited computing power and are unable to run powerful security functions. This leads to them having more software vulnerabilities as compared to other non-IoT devices.

Some of the reasons IoT devices have security vulnerabilities include:

* Poor access control
* Lack of computational capacity
* Lack of regular updates and software patches due to technical limitation or limited budget
* User negligence in updating IoT devices
* Inability to protect device from physical attack by a hacker. E.g., a criminal adding a chip or accessing device through radio waves.

1. **Unsecured Communication**

Most of the security mechanisms existing today were originally developed for desktop devices and are not as efficient when applied to IoT devices. One of the biggest threats resulting from unsecured communication within IoT networks is Man-in-the-Middle (MitM) attacks, where hackers can take control of your device, change its functionality, or install malware in it. The data exchanged between different IoT devices can also be read by cybercriminals if there is no encryption or the messages are in cleartext.

1. **Data Leakage from IoT Systems**

In addition to data leakage from IoT devices, hackers can also access data that is transferred and stored in the cloud. Cloud hosting services can experience attacks from external sources and include sensitive information like your bank account credentials, health records, and location.

1. **Malware**

According to a study by [Zscaler](https://ir.zscaler.com/news-releases/news-release-details/zscaler-study-confirms-iot-devices-are-major-source-security), devices that were at high risk of being hacked by malware were smartwatches, smart TVs, and set-top boxes. By injecting malware into an IoT system, cyber criminals can collect all data, meddle with the system’s functionality, and launch further attacks at other devices in the system.

1. **Cyber Attacks**

Apart from MitM and malware attacks, IoT systems are also susceptible to a number of other cyber attacks such as Denial of Service (DoS) attacks, device spoofing, application-based attacks, and physical intrusion, to name a few.

**Solutions to IoT Security Challenges**

By following IoT security solutions and best practices, we can ensure that the three main components of IoT are protected, i.e., network, data, and devices. Let’s look at some of the solutions.

1. **Secure your Smart Devices**

* Ensure that your devices are tamper-resistant by using camera covers or port locks. You can also apply strong boot-level password that disables the device in case of a tampering attempt.
* Device security and maintenance requires regular patches and updates. Establish regular automatic security updates for your devices.
* Conduct regular vulnerability assessments and penetration tests to detect vulnerabilities in your IoT firmware.

1. **Secure Your Network**

* Ensure strong authentication by using unique default credentials. Also use multi-factor authentication where possible.
* To ensure secure communication between network devices, enable encryption. You can also used optimized security protocols such as Secure Sockets Layer (SSL) and IPsec.
* Separate big networks into smaller ones to apply next-generation firewall security.
* Implement VPN for secure internet communication.
* Minimize your device bandwidth by limiting network traffic to the amount required for device functioning.

1. **Secure Your Data**

* Protect your sensitive data by using unique default password or requiring immediate password change after first use.
* Only collect data necessary for the functioning of your IoT system. This protects consumer privacy and lowers the risk of noncompliance with data protection standards and regulations.
* Secure your internal communications by restricting access to data within the IoT network.

**Conclusion**

It is important to think about privacy and security from early on when implementing an IoT system. However, it is difficult to implement robust security for IoT projects. Not only does it have hardware limitations, it also increases development time and cost, which is quite challenging for businesses. But with appropriate solutions and proactive measures in place, it is possible to overcome these challenges and implement secure IoT solutions.