The Business Leader's Guide to the

Internet of Things

Table of Contents

Introduction:
The Internet of Things (IoT)

The Internet of Things (IoT) is a network of interconnected "smart" devices (like sensors, cameras and machines) that are connected to the internet. These devices collect and exchange data and make decisions without the need for human intervention.

Devices within an IoT ecosystem are considered "smart" devices because of their autonomous and intelligent functions.

Benefits of using IoT technology

Boosts efficiency
IoT-powered machines can proactively identify threats and even schedule maintenance before a problem arises. This dramatically reduces downtime and increases efficiency.

Enhanced customer engagement
IoT enables businesses like yours to gather deep insights on your customers. You can use this data to tailor your recommendations, offer targeted promotions and create highly personalized interactions that make your customers feel special.

Better data collection and analytics
Gain access to a treasure trove of data, covering all the aspects of your business. Analyze this data to make smarter decisions, optimize operations and discover hidden opportunities for cost savings and revenue growth.

Streamlined inventory management
Track stock levels in real-time, forecast demand and build a robust inventory. IoT eliminates guesswork and gives you the power to avoid stockouts that irritate your customers and hurt your bottom line.

Components of IoT

The Internet of Things (IoT) is all about connecting devices and using their data to improve efficiency, gain deeper insights and automate tasks.

Let's explore the essential components that make this possible:

Hardware
Your hardware acts as your digital eyes and ears, capturing valuable data points. Think of a thermostat sensing temperature or a security camera detecting motion.

Connectivity
The hardware needs to be connected to the internet to share the data. Cellular networks and Wi-Fi serve as communication channels for transmitting information to the cloud.

Software
A powerful cloud-based software analyzes the collected data. It identifies trends, predicts potential issues and optimizes operations for you.

Interfaces
This is your command center. User-friendly mobile apps or dashboards provide insights and control, empowering you to interact with your connected devices effortlessly.

Here are some real-world examples

Smart printers
They can automatically detect when the toner is running out of ink and can order toner, saving you time and money.

Security cameras
They can send you an intruder alert when they detect motion, giving you complete peace of mind.

Smart thermostats
They can learn your heating and cooling preferences, saving you energy and money.

Inventory sensors
They facilitate timely decision-making and minimize stock-related challenges.

3 reasons IoT risks are expanding

Growing IoT technology adoption has opened the door for high-level security risks and threats, especially those that are tough to defend against because of flaws in many IoT devices.

These characteristics of IoT illustrate why risks and threats are prevalent:

IoT does not depend on human intervention to function — little to no oversight or accountability.

Multiple devices through an interconnected network collect, communicate, analyze and act on data.

A lot of sensitive data gets shared through IoT devices.

5 costly IoT security risks

Understanding IoT-related cybersecurity risks is crucial for protecting your business during its digital transformation.

Here are some common IoT security threats:

Denial-of-Service/Distributed Denial-of-Service (DoS and DDoS)

Imagine a restaurant swarming with fake customers placing endless orders. The restaurant staff gets overwhelmed and is unable to cater to the real customers. When DoS or DDoS attacks happen, hackers send endless requests to your devices, causing your network to slow down, crash or shut down.

Malware

Like a bad cold jumping between teammates, malware is a virus spreading through your devices, hijacking them to send malicious spam or even forming a "botnet" army that follows the hacker's command.

Passive wiretapping/Man-in-the-middle (MITM) attacks

You wouldn't want anyone to read your mail or eavesdrop on your phone calls. That's exactly what happens in an MITM attack. In this case, a malicious hacker intercepts the data flowing between your devices to steal sensitive information like passwords or confidential information.

Structured query language injection (SQL injection)

Visualize this as a supervillain injecting poison into the city's water supply to harm everyone. Similarly, a hacker injects malicious code to corrupt or destroy your data.

Evil twin attack

Imagine walking into your favorite coffee shop only to discover that it's a fake store that is set up to trick you into revealing your valuable information. Similarly, an evil twin attack creates a fake Wi-Fi network that looks like a trusted one, but its only purpose is to steal your login credentials when you connect.

5 common security risks that can exploit IoT vulnerabilities

1

Irregular patches and updates

Without regular patches and updates, hackers will eventually be able to exploit the weaknesses in your IoT devices. Often, many IoT device manufacturers don't deploy security patches regularly, giving cybercriminals ample time to crack the security protocols and access business-sensitive data. That's why it is a good idea to partner with a trusted IT service provider who ensures you are always protected.

2

Weak passwords

Your passwords are the key that keeps the thieves out. Don't make it easy for cybercriminals to steal your data by opting for easy passwords like 1234 or forgetting to reset the factory-set passwords. Regularly update your passwords and always choose something unique. This one simple step will save you from a world of pain.

Unsecure interfaces

Just securing your IoT device is not enough. It's important to also secure the web, application API, cloud and mobile interfaces. These interfaces can become easy targets without a strong authentication protocol.

3

4

Third-party applications

There are multiple third-party software applications available on the internet that you can integrate into the IoT ecosystem. However, installing such applications without caution could result in threat agents entering the system and corrupting your business data. In such cases, you should have a trusted IT expert to ensure that only reliable third-party applications are installed.

5

Skills gap

Not all businesses possess the required IT expertise to secure their IoT ecosystem. Without skilled professionals implementing robust cybersecurity defenses, cybercriminals can exploit your IoT devices and carry out cyberattacks. An experienced IT service provider can help bridge the skills gap without breaking the bank.

Best practices for managing IoT risks

Here are a few simple steps that can help you protect your connected devices:

- [ ] Conduct thorough and routine IoT risk assessments within your organization. Frequency — daily, monthly, annually — will depend on your unique business needs and risks.
- [ ] Automate routine patch management.
- [ ] Make sure third-party applications follow your security rules.
- [ ] Always assume that no device or network is fully secure and can be hacked.
- [ ] Use only trusted device IDs.
- [ ] Make it a policy requirement to store and lock IDs and credentials for IoT applications (especially extra sensitive ones) in secured (tamper-resistant) hardware with digital controls.
- [ ] Ensure only encrypted data is present within the IoT ecosystem (at rest and in transit).
- [ ] Deploy strict identity and access management policies.
- [ ] Develop a secure and risk-aware culture through consistent workforce training.
- [ ] Invest in technology for unified data protection, including backups and disaster recovery.
- [ ] Increase visibility into all networks and endpoints to minimize security gaps.

Having a trusted partner gives you peace of mind

Here is how an IT service provider can help you leverage IoT technology:

Builds an effective IoT strategy

An IT service provider can help you figure out how an IoT technology can boost your business and then find the right fit for your business without draining your budget.

Protects your data

An IT service provider keeps your data safe and sound by setting up secure communication protocols, implementing data encryption and safeguarding the system against cyberthreats.

Always keeps you updated

An IT service provider makes sure your connected devices are always working smoothly, troubleshoots any emerging issues and provides regular updates to maintain peak efficiency and security.

Keeps your business future-ready

An IT service provider helps you design a scalable IoT strategy tailored to adapt to your business growth. In addition to essential continuous training and support, the provider ensures seamless integration of new devices and flexible configuration adjustments.

Business leaders like you thrive on innovation. Don't be left behind. Seize the opportunity to revolutionize your business.

Let's connect to build your roadmap to success.

Tower23IT

Expertise · Solutions · Results