TECHSEVEN
PARTNERS

DISCOVER 7 COMMON INTERNET OF THINGS (IoT)

SECURITY GAPS THAT LEAD TO COSTLY DATA BREACHES

Contents

The Internet of Things (IoT): What Is It and What Are Its Benefits?

Put simply, the Internet of Things (IoT) is a network of interconnected devices that collect, share, process and act on data over a wireless network without any human intervention. The devices within an IoT ecosystem are considered "smart" devices because of their autonomous and intelligent functions.

3 Benefits of Using IoT technology

- Greater business agility via seamless collaboration
- Increased access to comprehensive datasets
- Proactive resolution of productivity issues via performance-based analytics

IoT Keeps Growing

Experts project that the total number of installed IoT-connected devices worldwide will amount to **30.9 billion units by 2025**.[1]

Components of IoT

Nearly all IoT solutions have four components at their foundation—hardware, connectivity, software and an interface.

Hardware

It can be a sensor or other devices. These sensors and devices collect data from the environment and perform actions.

Connectivity

The hardware needs to send and receive data to/from the cloud. You can achieve this with connectivity options like Wi-Fi, 5G, etc.

Software

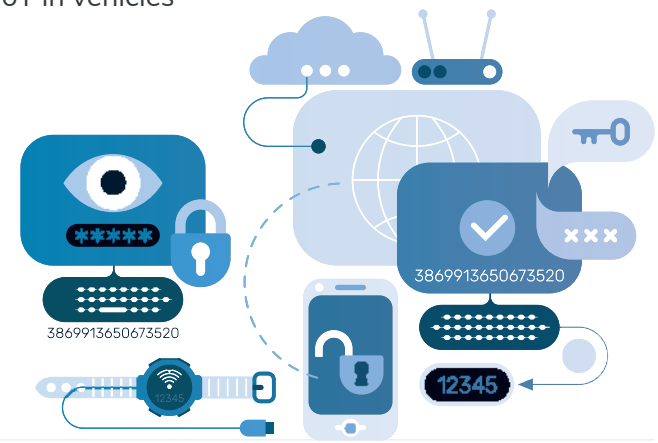
The software hosted in the cloud analyzes the data collected from the hardware and makes decisions.

Interface

An interface helps users interact with the IoT system. It can even be a mobile application interface that can turn a device on or off.

Examples of Business-Class IoT Technology

1. Printers and basic internet/Wi-Fi routers
2. Webcams (built-in/connected) and speakers/sound systems
3. Assistant devices
4. Smartwatches
5. “Smart” televisions and thermostats
6. Robotic floor cleaners
7. Traffic cameras/sensors and water/electrical meters
8. Connected IoT in vehicles



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.

More Devices
+
Automation
+
Mission-Critical Data

Exponentially Higher Risk

The Precarious State of IoT Security

About **60% of IoT devices** are vulnerable to medium- or high-severity attacks.[2]

Costly Security Risks That Come With IoT Technology

Having a thorough understanding of IoT cybersecurity problems and executing an effective strategy to mitigate risks can help shield your business and build confidence in your business' digital transformation process.

A considerable number of IoT attacks take place in the form of:

01 **Denial-of-Service/Distributed Denial-of-Service (DoS and DDoS)**
These attacks are common and easy to implement. When DoS or DDoS attacks happen, hackers flood the target system with multiple data requests, causing it to slow down, crash or shut down.

02 **Malware**
Malware attacks on an IoT ecosystem can cause significant damage. An entire network of devices can be hijacked to form a botnet that acts in accordance with the hacker's commands.

03 **Passive Wiretapping/Man-in-the-Middle (MITM) Attacks**
When an unauthorized entity breaks into an IT network and behaves as part of the network, data is at significant risk.

04 **Structured Query Language Injection (SQL Injection)**
SQL injection is a code injection technique in which hackers place malicious code in SQL statements. This technique can destroy databases.

05 **Evil Twin Attack**
An evil twin attack happens when a hacker sets up a fake Wi-Fi network that looks like a legitimate access point and tricks people into sharing their credentials.

7 Common Security Risks That Can Expose IoT Vulnerabilities

01

Lack of Regular Patches and Updates

While an IoT device may be secure at the time of purchase, hackers eventually detect new bugs and vulnerabilities. Only regular updates and patches can save a vulnerable device. However, many IoT device manufacturers deploy security patches irregularly. Therefore, cybercriminals get sufficient time to crack the security protocols and access business-sensitive data.

02

Insufficient Password Protection

Hard-coded and embedded credentials — such as pre-configured passwords set by manufacturers — provide an easy passageway for cybercriminals to enter business networks if they're not reset on a regular basis. When an entire product line has the same credentials (such as username: admin and password: admin), it creates a golden opportunity for hackers to exploit your network.

03

Unsecure Interfaces

Just securing your IoT device is not enough. Securing the web, application API, cloud and mobile interfaces is also important. Unsecured interfaces lacking strict authentication and authorization protocols play right into the hands of cybercriminals.

04

Usage of Vulnerable Third-Party Applications

There are multiple third-party software applications available on the internet that you can integrate into the IoT ecosystem. However, verifying their authenticity can be difficult. Installing such applications without caution could result in threat agents entering the system and corrupting the embedded database.

05

Improper Device Tracking

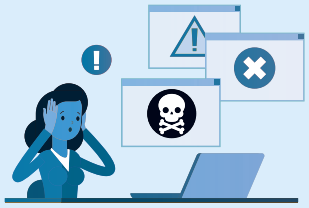
IoT manufacturers usually configure unique device identifiers to monitor and track devices. However, some manufacturers do not follow a standard security policy. In such cases, detecting suspicious online activity becomes difficult.

06

Inadequate Data Protection

There is a significant chance for data compromise when data collected by an IoT device moves across a network and gets stored in a new location. Lack of encryption or access control of business-sensitive data within the ecosystem (both at rest and in transit) invites hackers.

07



Skills Gap

If end users do not have sufficient knowledge about the IoT device, it can lead to a cyberattack. An untrained employee may be unaware that even connecting to an unsecured Wi-Fi network could turn into a security threat.

Global IoT Regulations & Shared Risks

Though there are laws in different parts of the world focusing on IoT security, including password hygiene, they lack effectiveness because:

- The laws are either vague or recently drafted. Conversely, IoT adoption is skyrocketing at an unprecedented pace.
- Cheap imports are available in the market but may not meet requirements outlined by existing laws.
- Manufacturers in their race to get a chunk of the IoT market can be careless when it comes to complying with security laws.

The Shared Risk of IoT Technology

- As of **December 2020, DDoS attacks for the year approximated 10 million** – the most DDoS attacks ever in a single year.[3]
- Over **95% of all IoT device traffic** is unencrypted.[2]
- About **72% of organizations experienced** an increase in endpoint and IoT security incidents last year and 56% of organizations anticipate a compromise via an endpoint or IoT-originated attack within the next 12 months.[4]

Strategies and Best Practices for Mitigating/Managing IoT Risks

Get the best out of IoT by following these best practices and strategies:

- 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.
- Include third-party systems in security policy management.
- Assume that no device or network is 100% secure. At any stage, a hacker could successfully attack a connected device or system.
- 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 within your workforce via consistent and frequent training programs.
- Invest in technology/solutions that deliver unified data protection through comprehensive backups, disaster recovery systems and business continuity strategies.
- Increase visibility into all networks and endpoints and work to minimize “silos” generated by growing attack surfaces.
- Immediately re-evaluate and work to reduce the attack surfaces that stem from supply chain risks.
- Implement systems/tools that provide ongoing network monitoring of your operational technology (OT) and IoT systems to detect or identify anomalous activity or warning indicators of advanced threats, both internally and externally.*
- Incorporate network segmentation practices into your IT/network/application configuration.

If these steps sound complicated or overwhelming, don’t worry. As a managed technology services provider, we can help your organization tackle these and many other security challenges.

*OT defines a specific category of hardware and software intended to monitor and control the performance of physical devices.

IoT Security Is Gaining Traction

Annual spending on IoT security measures will increase to **$631 million** in 2021.[5]

Having a Trusted Partner Gives You Peace of Mind

For SMBs, IoT provides an opportunity to augment business operations and become more productive.

It does not matter what your business size or industry is. You can use IoT in just about any environment. However, it is vital to be cautious about the vulnerabilities that come along with the technology. Also, the scope and scale of IoT deployments can seem overly complicated if not managed properly. That said, the vast benefits of using IoT technology make figuring out the security aspects worthwhile.

3 Benefits of Using IoT technology

- Greater business agility via seamless collaboration
- Increased access to comprehensive datasets
- Proactive resolution of productivity issues via performance-based analytics

Put our expertise and years of experience handling IoT security to work for your organization. To get an IoT security evaluation for your organization, contact us today. If IoT security gaps are found in your environment, we'll propose a comprehensive cybersecurity solution to address vulnerabilities and limit future risks. Get started now.

Contact us to learn more.
We can help make your IoT journey seamless and secure.

TECH SEVEN PARTNERS
803.327.6434
info@techsevenpartners.com

Sources:

1. Statista
2. 2020 Unit 42 IoT Threat Report
3. DARKReading
4. 2020 Endpoint and IoT Zero Trust Security Report
5. Forbes