



**GOVERNOR ERIC J. HOLCOMB'S
INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY**
302 West Washington Street, IGC-South, Room E208
Indianapolis, IN 46204

Author: Kemper, Grayson

Title: "How to Keep Company IoT Networks Secure"

Website: IoT For All Blog

Organization: IoT For All

Date: 30 September 2019

URL: <https://www.iotforall.com/internet-of-things-security/>

Accessed: 19 Oct 2019

Synopsis: As employees increase how often they use smart devices as part of their daily jobs, businesses are investing in building IoT networks.

While IoT networks make information accessible and protected from hardware errors, businesses should invest in the proper tools to keep their information safe.

Over 20 percent of companies reported a [data breach or cyberattack in 2018 that could be traced back to unsecured IoT devices](#), according to a Ponemon Institute Survey.

This article will focus on the approaches that help build a better [Internet of Things](#) security system and prevent a destructive breach.

Internet of Things Security - How to Keep Company IoT Networks Secure

Grayson Kemper



Illustration: © IoT For All

As employees increase how often they use smart devices as part of their daily jobs, businesses are investing in building IoT networks.

While IoT networks make information accessible and protected from hardware errors, businesses should invest in the proper tools to keep their information safe.

Over 20 percent of companies reported a [data breach or cyberattack in 2018 that could be traced back to unsecured IoT devices](#), according to a Ponemon Institute Survey.

This article will focus on the approaches that help build a better [Internet of Things](#) security system and prevent a destructive breach.

Bring Awareness to Risks of IoT for a Company

Many of the risks associated with IoT devices are distinct from other online security concerns.

Companies should invest time in learning how IoT devices could be putting their operations in jeopardy before deciding how to secure their network.

According to Forrester's [The State of IoT Security 2018](#), hackers' motives may not be associated with financial gain. The report states that IoT hackers tend to form centralized groups with a defined purpose.

Hacking an IoT device could mean accessing confidential company information on a security camera, a connected printer or supply chain machinery.

Because all devices in an IoT network are connected, these infiltrators can use this data to disrupt a company's entire operations and demand payment to restore functionality to a factory's machinery.

The More IoT Devices, The More Vulnerable Your Network

Each device in an IoT network represents an access point for hackers who may cross over from one device to another.

For example, in a [casino data leak](#), hackers breached an aquarium's temperature-control system to gain access to data about the casino's highest paying customers.

According to a [Business Insider report of the aquarium data leak](#), it's becoming more and more common for hackers to target IoT devices like thermostats to extract confidential data.

Research Proactive Security Measures to Implement

Your company can proactively avoid some data security risks of IoT networks.

A few ways to strengthen your company's IoT network include:

1. Learning about your network architecture
2. Reviewing supplier and partner security protocols
3. Leverage certifications

Learning About Your Network's Architecture

Companies can use their existing network management tools to survey their network.

A typical IoT network is a dynamic system with many moving parts and access points: The [devices and servers that make up a network](#) represent access points that are connected to several areas where confidential data can reside.

If your company understands its network architecture, it can figure out how to separate sensitive IoT networks from a business network to prevent a harmful data breach.

Reviewing Suppliers' and Vendors' Internet of Things Security

Protocols

Your suppliers' and vendors' devices could also facilitate a security breach at your company if they're connected to your network.

[Target's security breach](#), for example, happened because hackers gained access to a third-party vendor's unsecured HVAC system.

If your suppliers and vendors have IoT-enabled devices connected to your network, your network's safety could be at risk.

If you work closely with other businesses, it's a good idea to periodically survey your network with the goal of identifying atypical traffic patterns.

Leveraging Existing Certifications

In correlation with the rising IoT market, [IoT data certification programs](#) continue to emerge.

A reliable third party can monitor the authenticity of servers your IoT devices connect with and only allows connections with authenticated servers.

Checking with your suppliers and vendors to ensure they are using IoT security certifications is another smart safety measure.

Secure Personal Devices

You can also strengthen your individual device's resistance to bad actors through a few different approaches:

- Enable Two-Factor Authentication
- Implement Regular Updates
- Limit Secure Activity on IoT Devices

Enable Two-Factor Authentication

[Two-Factor Authentication](#) (2FA) confirms a user's identity using more than just a password and protect an IoT product from impersonation attacks.

For example, a hacker would need to learn a user's password and move past fingerprint, SMS message, or facial scan to gain access.

Beyond the security benefits, using a fingerprint or SMS message to confirm your identity is more efficient than entering log-in information.

If you forget your password, two-factor authentication allows you to quickly gain access to your device.

Update Software Regularly

Establishing a consistent maintenance schedule where you catch and implement software updates is crucial to securing IoT devices.

IoT devices are prone to security breaches partly because they're more challenging to patch than laptops and servers.

[Patch management is a growing industry](#) that your business should remain aware of if it plans to allow IoT devices to access its network.

Limit Activity on IoT Devices

It's important for employees to understand the risk their individual devices may bring to the office and make decisions accordingly.

If your company is deciding whether to opt for a smart printer, make sure the benefits outweigh the risks.

On an individual level, it's worth considering the implications of connecting smart devices to applications such as banking or insurance accounts.

Implementing a policy that limits the use of connected devices to highly-secured networks can reduce risk from personal error.

Awareness is the first step toward prevention when it comes to IoT data breaches.

Learn Ways to Protect Your Company's Data in an IoT System

Internet of Things security is necessary to safeguard both your business and your personal life from potential hackers.

Proactive measures to secure your data could include restructuring your network's architecture, adopting an IoT certification program or simply taking steps to secure your personal devices.

Your business should consider the risks seriously and then take action.