7 COMMON INTERNET OF THINGS (IoT) THREATS TO COMPLIANCE

Contents

The Internet of Things (IoT): Its Brief History and Benefits

Technically speaking, the Internet of Things (IoT) is the concept of connecting any device with an on/off switch to the internet and/or other connected devices – in such a way that the device(s) collect and share data about the way they are used and about the environment around them.[1]

- Today IoT has grown so much that **56 of 90 federal agencies** reported using IoT technology in 2020.[2]
- Also, experts project the total installed IoT-connected devices worldwide to amount to **30.9 billion** units by 2025.[3]

Components of IoT

When it comes to compliance, every device connecting to a “compliant” IT network must follow security protocols outlined by compliance regulations and liability insurance agreements. Overlooking any connected devices creates a non-compliance incident that could be exploited and used to harm your organization.

As you consider the impact of IoT in the work-from-home era, look into whether or not the following connected devices are in compliance with regulations you must follow to avoid costly fines:

Examples of IoT “smart” devices used in business:

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

IoT Regulation Challenges

Regulators cannot ignore data protection and privacy matters of technology like IoT because an enormous amount of data is generated, processed and shared by IoT environments.

Here are a few standards through which regulators view IoT:

HIPAA

Just like any other industry, healthcare is rapidly adopting IoT technology. The combination of medicine and IoT has led to the term, the Internet of Medical Things (IoMT). IoMT uses sensor capabilities, big data analytics, etc., to provide improved medical care. Also, cyberattacks targeted healthcare more than any other industry in 2020.[4] That's why a regulation like the Health Insurance Portability and Accountability Act (HIPAA) is essential.

One of the primary goals of HIPAA is to safeguard medical data, including Protected Health Information (PHI). You must inarguably comply with HIPAA if you are in the healthcare business.

GDPR

Most of the data-processing activities within the operational scope of IoT fall under the scrutiny of the European Union's General Data Protection Regulation (GDPR). Being GDPR compliant shows that the business has met basic data protection standards.

The GDPR covers both personal data and business-sensitive data. Therefore, it is vital for those who adopt IoT technology to be aware of the implications that the regulation will have on IoT devices, systems and applications.

CMMC

The new Cybersecurity Maturity Model Certification (CMMC) requirements established by the Department of Defense (DoD) aim to prevent Defense Industrial Base (DIB) cyberattacks.

CMMC is relatively new and might take a few years more to completely roll out. However, regardless of whether they use IoT or not, all contractors must gear up for CMMC to avoid any last-minute hitches.

A single IoT device that does not comply with the law can invalidate your cyber insurance claims. Being compliant comes with a lot of benefits—you can improve overall data safety, avoid potential criminal charges, improve public relations, prevent attrition and ensure insurance providers pay out cyber insurance claims in the event of an incident. If you have implemented a Bring Your Own Device (BYOD) policy within your business, you might have to evaluate the situation to ensure everything is compliant.

Compliance Keeps These in Check

- About **60% of IoT devices are vulnerable to medium- or high-severity** attacks.[5]
- Over **95% of all IoT device traffic is unencrypted**.[5]
- **About 72% of organizations experienced an increase in endpoint and IoT security** incidents last year and 56% of organizations expect a compromise via an endpoint or IoT-originated attack within the next 12 months.[6]

7 IoT-Related Risks and Threats

Protecting data integrity and privacy against the growing risk of IoT device attacks has become a global priority. Here are some IoT-related risks and threats you'll want to guard your devices against:

Hackers exploit vulnerabilities in IoT devices and use them to access the entire network.

Lack of proper security controls:

- Even if software flaws are detected, you may not be able to patch an IoT device on time with security updates, leaving it exposed to risks.
- Many Operational Technology (OT) systems are flat, lacking filtering choke points such as firewalls or router ACLs. It renders standard network remediation tactics ineffective when it comes to preventing the spread of malware and can sometimes trigger critical infrastructure disruptions/failures.
- Most IoT networks lack even basic encryption systems for data in transit and data at rest.

- Some sensors collect (and potentially store and share) sensitive data without the user's knowledge or permission. This could lead to industrial espionage and eavesdropping.

- There are no universal regulatory requirements or "standards" for manufacturing or security for IoT.

- Default password vulnerabilities are still a primary concern.

- IoT ecosystems are complex. A key challenge is that a "one size fits all" security policy or solution is not realistic or currently achievable.

- The lack of broad universal knowledge and awareness of IoT at the user level regarding functionality and risks.

- The wave of modern, connected, medical devices shows promise in improving patient care, gathering better clinical data, improving efficiency and reducing costs. However, they also come with the baggage of security risks, threats and vulnerabilities from technology, software, cloud and human factors. In addition:

  - Most medical devices run on commercial off-the-shelf (COTS) software like Linux, Windows and Oracle, which exposes them to the same vulnerabilities that those programs already have.

  - Manufacturers are still regularly using old technologies that do not comply with modern digital landscape requirements.

IoT Compliance Regulations

With a focus on IoT-related consumer protection, government authorities from different countries are attempting to regulate this technology. Many regulatory bodies at the state and federal levels have drafted IoT security bills designed to hold product manufacturers accountable for consumer device security. This new wave of IoT regulations is prompting manufacturers to consider ways to enhance their device security programs to include business-grade and enterprise-level IoT security features.

Here's a list of country-specific regulations and initiatives:

United States

- Federal IoT Cybersecurity Improvement Act (Law: December 4, 2020)
- There are two additional state-sanctioned bills, which are:
  1. The SB-327 from California, also known as the "IoT bill."
  2. The state of Oregon's bill relating to security measures required for devices connected to the internet.

Canada

- Canadian Multistakeholder Process: Enhancing IoT Security initiative

Europe/EU

- The EU Cybersecurity Act (2019)

Japan

- Basic Act of Cybersecurity & New Cybersecurity Strategy (2018)
  – This cybersecurity guidance released by the Japanese government includes 51 references to use cases and best practices for IoT.

Components of the Global Regulation Wave Surrounding IoT Product Security

According to the new wave of regulations, all IoT device manufacturers will have to comply with the components below if they want to stay off regulator radars:

01 **Prioritize Governance**
There must be effective governance to promote standardization. Regularly monitoring regulatory risks is also essential.

02 **Conduct Thorough Risk Assessment**
It is crucial to detect the risks posed by connected devices to your organization's operations/assets and stakeholders, including customers.

03 **Configuration Management**
Standardize configuration management to ensure the best configuration is present in IoT devices.

04 **Identity Management and Access Control**
Only authorized people should have access to IoT devices, data and networks.

05 **Data Management and Privacy**
Manufacturers are responsible for implementing methods to protect data generated, stored and transmitted by the devices.

06 **Vulnerability Monitoring and Patching**
Regularly monitor, detect and resolve security problems in the devices.

Can your business afford to continue to use non-compliant IoT devices?

The Cost of Ignoring IoT Compliance Risks

If you are under the impression that you can get away with not complying with regulations, you are mistaken. Keep in mind that being non-compliant can land your business in hot water via:

01 **Hefty penalties**

HIPAA violations can draw fines ranging from $100 to $50,000 per violation, with a maximum fine of $1.5 million per calendar year of non-compliance.[7] GDPR violations lead to hefty violation fines worth 2% to 4% or more of company turnover based on the severity of neglect.[8]

02 **Uninvited audits**

Non-compliance can lead to unpleasant inspections and audits that can lead to fines.

03 **Denial of cyber insurance claims**

Be extra careful when selecting IoT solutions for your business. Using a single non-compliant solution can cause your insurance provider to deny a cyber insurance claim.

04 **Loss of business reputation**

Remember, it takes years to build a reputation and just minutes to ruin it.

05 **Imprisonment or even forced closure**

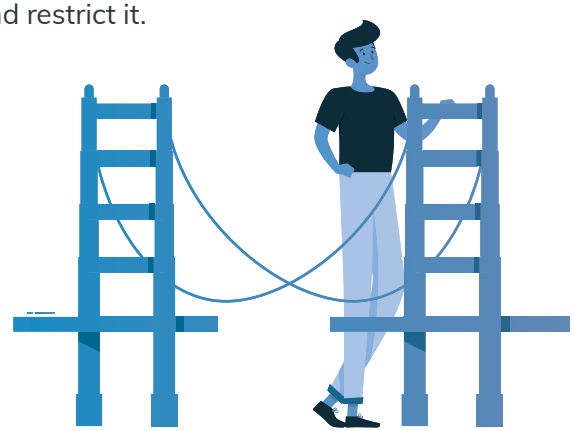
In cases of severe non-compliance, regulatory bodies can sanction the arrest of top executives or even close the business.

Is your business prepared to deal with any of the above?

How to Bridge IoT Compliance Gaps

A robust compliance framework must consider the following in the security audit checklist:

- Update all passwords to increase their strength and use multifactor authentication if possible. Avoid devices with hard-coded passwords and always check permissions granted for devices.
- Strictly review the security features and privacy policies of the IoT applications and backend services.
- Always place IoT devices on a firewalled and monitored network. It helps you keep network traffic in check.
- Turn off unnecessary functionalities of IoT devices. This includes physically blocking cameras, microphones, etc.
- Restrict automatic connections via Wi-Fi and other connectivity options. Doing so helps keep device infiltration in check.
- If incoming traffic is not blocked, check for open software ports that permit remote access and restrict it.
- Only buy devices that support encryption. Consider using a VPN.
- Closely check the lifecycle of the devices so that you can remove any outdated products.



Partner for Compliance Success

You can also choose a Compliance as a Service (CaaS) offering from a partner like us. We can help you with your compliance matters so you can concentrate on your business.

We'll run a comprehensive network assessment to see if your IoT network is robust and secure. Beyond just the network, we can do a 360-degree compliance health check for HIPAA, GDPR, CMMC, NIST CSF and cyber liability insurance.

We can help you:

- Run comprehensive risk assessments
- Automate compliance documentation
- Implement ongoing monitoring for vulnerabilities or threat indicators
- Get expert technical support and consultation services
- Safeguard your data from the evolving threat landscape
- Get insightful reports
- Maintain a commitment to an effective compliance strategy

Start your journey towards compliance for IoT technologies. Contact us now to set up a consultation or assessment!

Sources:

1. IBM
2. US GAO-20-577 Report
3. Statista
4. IBM Cost of Data Breach Report
5. 2020 Unit 42 IoT Threat Report
6. 2020 Endpoint and IoT Zero Trust Security Report
7. National Library of Medicine
8. GDPR Associates