# Security for Internet of Things Device Manufacturers

The Internet of Things (IoT) has introduced new security risk factors that are unprecedented in scope and scale. Although the recommendations presented here are intended for IoT manufacturers, many of them are equally applicable to other stakeholders in the IoT community, such as service providers and software developers. From the perspective of manufacturers, securing IoT requires answers to the following questions:

- To what risk factors are IoT stakeholders exposed?
- Why and how are IoT devices impacted?
- What are the latest laws and guidelines that affect IoT manufacturers?
- How can IoT manufacturers secure their devices and customers' data?

> "SECURITY VULNERABILITIES IN IOT PRODUCTS CAN EXPOSE MANUFACTURERS TO SERIOUS CYBERSECURITY RISK, POTENTIALLY RESULTING IN REPUTATIONAL DAMAGE AND HEAVY FINES."

According to two recent surveys, top executives consider building trust and ensuring cybersecurity in IoT deployment the most essential considerations.[1, 2] A significant portion of the revenue derived from an IoT-driven economy is produced through monetization of the data generated from the IoT ecosystem.[3] Once data are part of the equation, security and privacy naturally become important considerations.

## The Current State of IoT Security

In the past, consumer gadgets or industrial devices were designed primarily to provide the necessary functionality and performance. They were produced at the lowest cost and were brought to market as quickly as possible. These devices or software often lacked the basic mechanisms to protect themselves against misuse or hacking.

Recent IoT-related security incidents range from the massive, such as the Internet blackout caused by the Mirai attack in 2016,[4] to specific attacks, such as the security compromise of a digital thermometer in a fish tank.[5] These kinds of attacks affect not just the commercial sector but also household consumers, as evidenced by the Jeep hack in 2015[6] and the hack of Internet-connected smart toys in 2017.[7]

Security vulnerabilities in IoT products can expose manufacturers to serious cybersecurity risk, potentially resulting in reputational damage and heavy fines. Another issue that demands attention is counterfeiting. Counterfeit products pose an immediate and tangible threat to manufacturers in economic terms through the loss of revenue. For

**Welland Chu,** Ph.D., CISA, CISM
Is the business development director, Asia and Pacific Region, at the cloud protection and licensing business unit of Thales. He serves as the secretary and vice president of certification at the ISACA® China–Hong Kong Chapter. During his 26 years in the security industry, Chu has led teams of security professionals in assessing and implementing security solutions for clients in the critical infrastructure sector. He can be reached at Welland.Chu@thalesgroup.com.

example, the semiconductor industry estimates that between US$75 billion and US$169 billion worth of counterfeit semiconductor parts are currently circulating in the marketplace.[8] Because of the uncertainty of the behavior of these counterfeit products, the confidentiality, integrity, availability (CIA) triad may be impacted where the data stored, transmitted or processed in the system may be subject to accidental or unauthorized storage, processing, access, destruction, alteration, loss or lack of availability during the life cycle of the IoT components. If the IoT industry is aware of the damage caused by this lapse in security, why are manufacturers and users of IoT devices not doing more to mitigate these security threats?

One of the challenges facing security experts and manufacturers is that the IoT ecosystem is complex and presents a large attack surface. The situation is complicated by the fact that IoT devices are traditionally not cyberresilient, and they have long life spans (typically greater than 10 years). Finally, the need to physically go on-site and manually replace IoT devices often deters operators from conducting the necessary maintenance, even when a serious vulnerability has been identified.

## Regulations and Guidelines

Recognizing the importance of security and the long-term implications of flawed IoT devices, the US Senate,[9, 10] the US State of California,[11] and the US Food and Drug Administration[12, 13] have spearheaded efforts to regulate IoT security. On the other side of the Atlantic, the European Parliament[14] and the Department of Digital, Culture, Media and Sport in the United Kingdom[15] have issued regulations and guidelines that govern the security of IoT. **Figure 1** summarizes the applicable EU and US laws and their impacts on IoT business stakeholders.

**Figure 1—US and EU Cybersecurity Laws**

| Law | Effective Date | Who Is Affected? | Key Points |
|---|---|---|---|
| US IoT Cybersecurity Improvement Act of 2019 | Pending* | IoT contractors and vendors selling to the US government | • High visibility, with director-level involvement by US Department of Homeland Security, NIST, US Office of Management and Budget (OMB)<br>• Does not contain any known security vulnerabilities or defects<br>• Firmware properly authenticated and trusted |
| California Senate Bill No. 327 | 1 January 2020 | IoT manufacturers selling in California | • Manufacturers are responsible for protecting the device and any information contained therein<br>• User must generate a new means of authentication before access (i.e., no fixed password) |
| US Food and Drug Administration Premarket and Postmarket Management of Cybersecurity | 2014, 2016 | Medical device manufacturers | • Security requirements must be addressed during design, manufacturing, implementation and operation phases<br>• Verification and validation for software updates and patches |
| Regulation (EU) 2019/881 on ENISA and on Information and Communications Technology Cybersecurity Certification | 27 June 2019** | Manufacturers or providers of products, services or processes of IoT*** | • A European cybersecurity certification scheme shall be established<br>• Security of protecting the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data will be attested against assurance levels of "basic," "substantial" or "high" in accordance with the level of the risk associated with the intended use<br>• Only authorized persons, programs or machines are able to access the data, services or functions<br>• Software and hardware are provided with mechanisms for secure updates |

* The bill is currently being reviewed and amended by various US Senate committees. When the review process is complete, the bill will be voted on by the Senate and, if approved, sent to the US House of Representatives. If approved by both houses of Congress, the bill will be sent to the President to be signed into law.

** While the regulation has been enacted, the European cybersecurity certification scheme, which is required under the regulation, is yet to be developed. Certification against the scheme will be voluntary initially but may gradually become mandatory in the European Union for critical products or processes.

*** The regulation covers information and communications technology, which encompasses IoT.

In addition to publications by the US Department of Homeland Security[16] and the US National Institute of Standards and Technology (NIST),[17, 18] guidelines have been published by other bodies and industry associations. Because the IoT touches on many disciplines and is applied at different levels, some IoT security guidelines are written for a specific industry,[19, 20, 21] while others are more generally applicable.[22, 23]

## IoT Security Framework

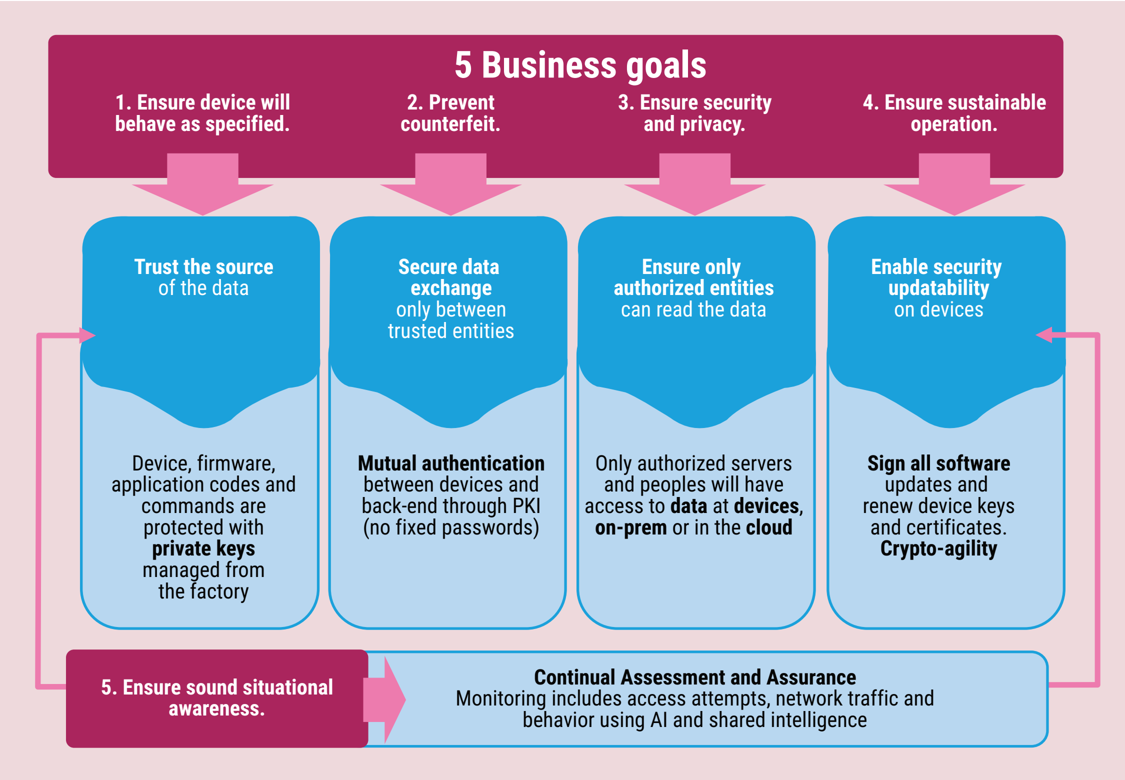
It would be highly desirable to adopt one baseline security framework, but unfortunately, there is no one-size-fits-all solution to IoT security. The security framework adopted by most security-conscious practitioners is the NIST Cybersecurity Framework (CSF).[24] The following sections explain how some well-proven technical measures can be implemented to achieve security and privacy by design, thereby enabling manufacturers to identify threats and protect against them. This helps service operators detect, respond and recover in the operation phase more effectively and efficiently.

### Five Key Principles of IoT Security

The five key principles of IoT security are summarized in **figure 2.** If these principles are followed, the business goals of IoT device manufacturers will be aligned with security and compliance requirements. These requirements can be met when the relevant technological and procedural controls are in place.

1. Ensure that devices function only as specified:
   - Devices accept only authorized, trusted data from trusted sources.
   - Devices will not run unauthorized firmware or application codes, including malware.
   - Unauthorized commands cannot run in devices.
2. Prevent counterfeits from running in the system:
   - Only trusted devices can be connected and communicated with.
   - Devices, software codes and commands are mutually authenticated.
   - Software, including firmware and application codes, cannot be illegally copied.
   - There is no fixed password.

Figure 2—The 5 Key Principles in IoT Protection


5 Business goals
1. Ensure device will behave as specified.
2. Prevent counterfeit.
3. Ensure security and privacy.
4. Ensure sustainable operation.
Trust the source of the data
Secure data exchange only between trusted entities
Ensure only authorized entities can read the data
Enable security updatability on devices
Device, firmware, application codes and commands are protected with private keys managed from the factory
Mutual authentication between devices and back-end through PKI (no fixed passwords)
Only authorized servers and peoples will have access to data at devices, on-prem or in the cloud
Sign all software updates and renew device keys and certificates. Crypto-agility
5. Ensure sound situational awareness.
Continual Assessment and Assurance
Monitoring includes access attempts, network traffic and behavior using AI and shared intelligence

3. Ensure security and privacy:
   - Only authorized entities can read data intended for them.
   - Data security and privacy are protected in accordance with international standards such as the EU General Data Protection Regulation (GDPR) and industry-specific standards such as the Payment Card Industry Data Security Standard (PCI DSS).
   - Protection extends to the edge and in the cloud.
4. Ensure sustainable operation:
   - Security is updatable on devices.
   - Firmware and application codes are updated and cryptographically signed.
   - Crypto-agility is built into devices and at the back end for postquantum operation.[25]
   - There is automated operation with no human intervention.
5. Ensure sound situational awareness:
   - Continual assessment and assurance are performed.
   - Monitoring includes access attempts, network traffic and behavior with the help of artificial intelligence (AI) and shared intelligence.

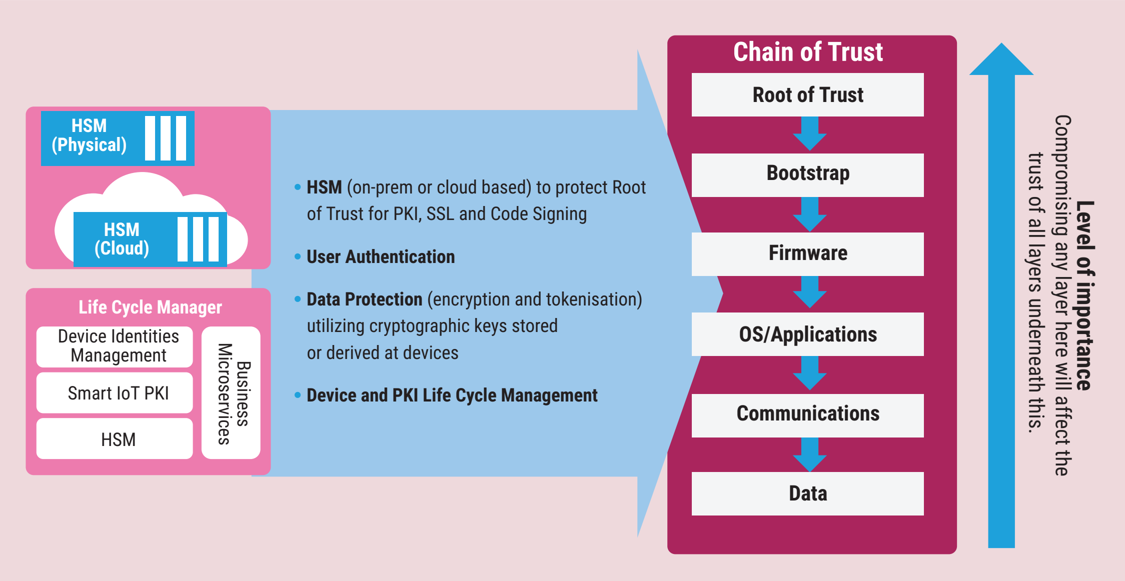
By following these principles, IoT devices and systems can defend themselves against cybersecurity risk.

## Protecting the Chain of Trust

Public key infrastructure (PKI) is the technology that enables the mutual authentication of devices and codes. This ensures that only authorized devices, firmware and application codes can run in a system. This technology also supports subscriber identity module (SIM)-based security.[26] The idea is that each entity in the system (this includes the IoT hardware, bootstrap, firmware and application code) is given a unique digital certificate signed by a trusted party. The signing process is usually performed during the manufacturing stage using the manufacturer's private key. When a device needs an update and firmware is going to be loaded into the device, the firmware and the device mutually authenticate each other based on the signed certificates before the firmware is accepted and loaded. Similarly, communications between devices are cryptographically protected (via cryptographic signature and encryption), so that only authorized devices can communicate with each other and hackers or other unauthorized parties cannot eavesdrop on the communications.

Clearly, protecting the chain of trust (**figure 3**) and the cryptographic signing keys is critical in any IoT system. The private keys of IoT devices can usually be protected within the enclave of the machine control unit.[27] Manufacturers can centrally generate cryptographic keys before loading them into devices

Figure 3—Protecting the Chain of Trust


HSM (Physical)
HSM (Cloud)
Life Cycle Manager
Device Identities Management
Smart IoT PKI
HSM
Business Microservices
• HSM (on-prem or cloud based) to protect Root of Trust for PKI, SSL and Code Signing
• User Authentication
• Data Protection (encryption and tokenisation) utilizing cryptographic keys stored or derived at devices
• Device and PKI Life Cycle Management
Chain of Trust
Root of Trust
Bootstrap
Firmware
OS/Applications
Communications
Data
Level of importance
Compromising any layer here will affect the trust of all layers underneath this.

as part of the device provisioning process. The equipment deployed for this task should follow industry standards, such as using US Federal Information Processing Standards (FIPS)-certified hardware security modules (HSMs).[28] For ease of deployment and to cater to sudden increases in usage, IoT manufacturers may explore the on-demand services offered by trusted service providers.[29]

> “PROTECTING THE CHAIN OF TRUST AND THE CRYPTOGRAPHIC SIGNING KEYS IS CRITICAL IN ANY IOT SYSTEM.”

## Conclusion

Manufacturers can demonstrate due care and win customer trust by following the security design described previously. Security at the IoT device level is attainable, and prevention is the best option. By protecting the chain of trust, IoT can defend itself, and manufacturers and operators can minimize losses from counterfeits, attain regulatory compliance, minimize misuse and facilitate future maintenance. Such protection covers device hardware, firmware and application codes and the data they process. Finally, cybersecurity and privacy risk factors should be assessed and mitigated throughout the product life cycle.

## Endnotes

1 PricewaterhouseCoopers (PWC), “2019 IoT Survey: Speed Operations, Strengthen Relationships and Drive What’s Next,” *https://www.pwc.com/us/en/services/consulting/technology/emerging-technology/iot-pov.html#about-survey*

2 AT&T, *AT&T Cybersecurity Insights Report, 2019/2020 Edition*, *https://cybersecurity.att.com/resource-center/analyst-reports/cybersecurity-insights-report-ninth-edition*

3 Russo, M.; M. Albert; “How IoT Data Ecosystems Will Transform B2B Competition,” BCG Henderson Institute, 27 July 2018, *https://www.bcg.com/publications/2018/how-internet-of-things-iot-data-ecosystems-transform-b2b-competition.aspx*

4 Hilton, S.; “Dyn Analysis Summary of Friday October 21 Attack,” Dyn, 26 October 2016, *https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/*

5 Schiffer, A.; “How a Fish Tank Helped Hack a Casino,” *The Washington Post*, 21 July 2017, *https://www.washingtonpost.com/news/innovations/wp/2017/07/21/how-a-fish-tank-helped-hack-a-casino/?utm_term=.09f1f239b5dc*

6 Greenberg, A.; “The Jeep Hackers Are Back to Prove Car Hacking Can Get Much Worse,” *Wired*, 1 August 2016, *https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/*

7 Frenkel, S.; “A Cute Toy Just Brought a Hacker Into Your Home,” *The New York Times*, 21 December 2017, *https://www.nytimes.com/2017/12/21/technology/connected-toys-hacking.html*

8 McKeefry, H. L.; “Counterfeits Costing Semiconductor Industry Billions,” EET Asia, 14 March 2019, *https://www.eetasia.com/news/article/Counterfeits-Costing-Semiconductor-Industry-Billions*

9 Govtrack, “S. 734: Internet of Things Cybersecurity Improvement Act of 2019,” 23 September 2019, *https://www.govtrack.us/congress/bills/116/s734*

10 Govinfo, “Senate Committee on Homeland Security and Governmental Affairs Report on S.734,” 23 September 2019, *https://www.govinfo.gov/content/pkg/CRPT-116srpt112/pdf/CRPT-116srpt112.pdf*

11 California Senate, “SB-327 Information Privacy: Connected Devices,” USA, *https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327*

12 US Food and Drug Administration, “Content of Premarket Submissions for Management of Cybersecurity in Medical Devices,” 2 October 2014, *https://www.fda.gov/media/86174/download*

13 US Food and Drug Administration, “Postmarket Management of Cybersecurity in Medical Devices,” Guidance for Industry and Food and Drug Administration Staff, 28 December 2016, *https://www.fda.gov/media/95862/download*

[14] Official Journal of the European Union, Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No 526/2013 (Cybersecurity Act), 17 April 2019, *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN*

[15] Department of Digital, Culture, Media and Sport in the UK, "UK Code of Practice for Consumer IoT Security," 14 October 2018, *https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security/code-of-practice-for-consumer-iot-security*

[16] US Department of Homeland Security, "Strategic Principles for Securing the Internet of Things Version 1.0," 15 November 2016, *https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf*

[17] National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity Version 1.1," USA, 16 April 2018, *https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf*

[18] National Institute of Standards and Technology, "Security and Privacy Controls for Federal Information Systems and Organizations Revision 4," Special Publication (SP) 800-53, USA, April 2013, *http://dx.doi.org/10.6028/NIST.SP.800-53r4*

[19] Groupe Speciale Mobile Association (GSMA), "CLP.11—IoT Security Guidelines Overview Document Version 1.0," 8 February 2016, *https://www.gsma.com/iot/wp-content/uploads/2016/02/CLP.11-v1.1.pdf*

[20] International Society of Automation (ISA), "New ISA/IEC 62443 Standard Specifies Security Capabilities for Control System Components," *InTech Magazine*, September–October 2018, *https://www.isa.org/intech/201810standards/*

[21] Heyl, J.; "UL2900 Overview," October 2017, *https://cybersecuritysummit.org/wp-content/uploads/2017/10/4.00-Justin-Heyl.pdf*

[22] IoT Security Foundation, "Secure Design Best Practice Guides Release 2," November 2019, *https://www.iotsecurityfoundation.org/wp-content/uploads/2019/11/Best-Practice-Guides-Release-2.pdf*

[23] ISACA®, *Assessing IoT Internet of Things: Upsides, Downsides and Emerging Ethics*, USA, 2017, *https://www.isaca.org/bookstore/bookstore-wht_papers-digital/whpaiot*

[24] *Op cit* NIST 2018

[25] Thales, "Quantum Computing and Cybersecurity," 23 October 2019, *https://www.thalesgroup.com/en/germany/magazine/quantum-computing-and-cybersecurity*

[26] GSMA, "Common Implementation Guide to Using the SIM as a 'Root of Trust' to Secure IoT Applications," 3 December 2019, *https://www.gsma.com/iot/wp-content/uploads/2019/12/IoT.04-v1-Common-Implementation-Guide-1.pdf*

[27] Microsoft, "Seven Properties of Highly Secure Devices," March 2017, *https://www.microsoft.com/en-us/research/wp-content/uploads/2017/03/SevenPropertiesofHighlySecureDevices.pdf*

[28] National Institute of Standards and Technology, "Cryptographic Module Validation Program," USA, 11 October 2016, *https://csrc.nist.gov/Projects/cryptographic-module-validation-program*

[29] Gemalto, "SafeNet Data Protection on Demand," *https://safenet.gemalto.com/data-protection-on-demand/*