KPMG

After the rainfall of IoT regulations

New regulations are making IoT product manufacturers responsible for safeguarding consumers on the IoT. Are they ready?

kpmg.com

About the authors

Mike Krajecki

Managing Director, Emerging Technologies
KPMG LLP

Mike is a managing director in KPMG's Emerging Technologies practice. He has over 12 years of professional experience and has led the development of KPMG's Internet of Things (IoT) risk and governance service offering and supporting framework. Mike specializes in helping organizations identify, assess, and manage risks related to smart, connected products and digital assets. He has IoT delivery experience in automotive, consumer products, public transit, medical devices, and industrial. He also holds CPA and CISA certifications.

Danny Le

Principal, Cyber Security Services
KPMG LLP

Danny is a principal in KPMG's Cyber practice, specializing in cybersecurity. With significant international consulting experience, he has helped some of the world's largest companies manage global technology and regulatory risk across multiple jurisdictions and business operations. Danny spearheaded the development of KPMG's capabilities in information security protection and business resilience. He has deep knowledge of leading practices in technology risk management, internal controls, business processes, governance, and reporting in a wide range of industries.

Nick Naddaf

Manager, Emerging Technologies
KPMG LLP

Nick is a manager in KPMG's Emerging Technologies practice specializing in digital strategy and governance, enterprise IoT and mobile risk and security, and IT internal audit. He has worked with some of the nation's leading organizations in the manufacturing, healthcare, pharmaceutical, agriculture, and professional services industries to assess digital risks and improve digital risk management and governance.

Rules are being written

The Internet of Things (IoT) has already reshaped the world as we know it. And it only continues to expand. According to IHS Markit, IoT devices are expected to surpass 125 billion by 2030. The consumer sector—made up of now-pervasive products like smart home appliances, connected vehicles, personal fitness devices, and digital health tools—will account for nearly two-thirds of the total.[1]

By constantly collecting and using valuable data, IoT products make life more effortless for consumers, delivering greater convenience, enhanced experience, and more responsive services. Focusing on their many benefits, it's easy to understand their proliferation. And it's easy to overlook the risks.

But the reality is, risks abound. Undersecured connected devices can expose and compromise consumers' physical and financial health and personal privacy, doing even more damage than traditional technologies that do not interact with the physical world. Over the past few years, hackers have hijacked connected consumer gadgets like smartphone apps, webcams and wireless routers, and even internet-capable thermometers and Bluetooth-enabled toys. The results were significant. IoT device hacks have allowed malicious actors to knock websites offline and render much of the internet useless,[2] eavesdrop on conversations and spy on people in their homes,[3,4] flood people with clickbait to earn a profit[5], steal sensitive personal data,[6] and do plenty of other damage.

Given the massive potential financial and reputational damage caused by a breach, manufacturers have a strong incentive to make safe, secure connected consumer products. Safe and secure IoT devices are important to building customer trust in the product and the brand. Manufacturers that miss the mark on product security and privacy risk losing market share to competitors who get it right.

But still, failures happen. Lawmakers want them to stop. With consumer protection as the end goal, government authorities around the world are leading the charge to regulate the IoT—and they've set their sights on manufacturers. The regulatory pipeline at the state, federal, and global level is chock full of IoT security bills designed to hold product manufacturers accountable for consumer device security.

The current regulatory landscape makes it clear that the onus will be on manufacturers to protect consumers from exposure and harm from IoT devices. The burden will fall on manufacturers to not only enhance consumer experiences via IoT, but also make sure they are safe and protected during the journey.

---

[1] Number of Connected IoT Devices Will Surge to 125 Billion by 2030, IHS Markit Says (IHS Markit, Oct. 24, 2017)

[2] The Mirai botnet explained: How teen scammers and CCTV cameras almost brought down the internet (CSO, March 9, 2018)

[3] This pretty blond doll could be spying on your family (*Washington Post*, Feb. 23, 2017)

[4] Internet of Babies–When baby monitors fail to be smart (SEC Consult, Feb. 21, 2018)

[5] Hackers Take Over IoT Devices to 'Click' on Ads (ThreatPost, May 9, 2019)

[6] Hackers once stole a casino's high-roller database through a thermometer in the lobby fish tank (Business Insider, April 15, 2018)

Snapshot of IoT security regulations

A wave of IoT security regulations on manufacturing companies is coming at both the federal and state levels. Rules requiring manufacturers to equip IoT devices with minimum reasonable security standards are already signed into law in a handful of U.S. states. Two bills (in California and Oregon) have already been passed. Multiple bills have been proposed at the state level and are currently working their way through the state legislative systems. And numerous bills have been introduced to U.S. Congress.

Manufacturers that sell connected products on global scale—and in today's connected world, most do—must also track a variety of passed and pending laws around the world, including voluntary cross-industry guidance and standards that aren't legally enforceable but that may set the precedent for future legislation. Numerous foreign regions and countries where U.S. manufacturers frequently do business—including the European Union, United Kingdom, China, Japan, Australia, Canada, and Brazil—have their own version of legislation either passed or in the works.

Some manufacturing industry subsectors are also governing themselves by developing IoT security standards specific to those industries. The automotive industry has collaborated to design best practices for securing connected vehicles and the healthcare industry has worked in partnership to improve the overall security of medical devices by setting guidelines for design controls, patching, and incident response. An electronics safety group is currently developing an IoT device cybersecurity rating system based on a checklist of capabilities and requirements. Functioning as a kind of seal of approval, the ratings will help consumers gauge the safety and security of IoT products and give manufacturers the opportunity to differentiate themselves in the marketplace.

Finally, it's not only new regulations and guidelines that are impacting product manufacturers. Regulators are also applying several existing security and privacy laws to IoT devices and platforms. For example, makers of connected devices that use consumer health information are subject to Health Insurance Portability and Accountability Act (HIPAA) data privacy requirements. In addition, smart toy makers must comply with the Children's Online Privacy Protection Act (COPPA), which regulates the data collection practices of online services directed to children.

Overview of IoT security regulation[7]

United States, federal level

— Multiple pending bills in the U.S. Senate and the House of Representatives

United States, state level

— Information Privacy: Connected Devices (State of California)

— Relating to Security Measures Required for Devices that Connected to the Internet (State of Oregon)

— Pending bills in multiple U.S. states including Illinois, Maryland, Massachusetts, New York, Vermont, and others

China

— Circular on Comprehensively Advancing the Construction and Development of Mobile Internet of Things (Ministry of Industry and Information Technology)

Japan

— IoT Acceleration Consortium (Ministry of Internal Affairs and Communications; Ministry of Economy, Trade and Industry)

United Kingdom

— Code of Practice for Consumer IoT Security (UK Department for Digital, Culture, Media & Sport)

Canada

— Enhancing IoT Security Initiative (Internet Society)

Brazil

— The National Plan for the Internet of Things (Ministry of Science, Technology, Innovation and Communications; National Telecommunications Agency)

European Union

— ETSI TS 103 645 (European Telecommunications Standards Institute)

Australia

— IoT Reference Framework (Internet of Things Alliance Australia)

Snapshot of recent industry-specific regulatory activities

— Automotive Cybersecurity Best Practices (Automotive Information Sharing and Analysis Center)

— NHTSA Cybersecurity Best Practices for Modern Vehicles (National Highway Traffic Safety Administration)

— Medical Device Safety Action Plan (U.S. Food and Drug Administration)

— 21 CFR Part 820.30 (U.S. Food and Drug Administration)

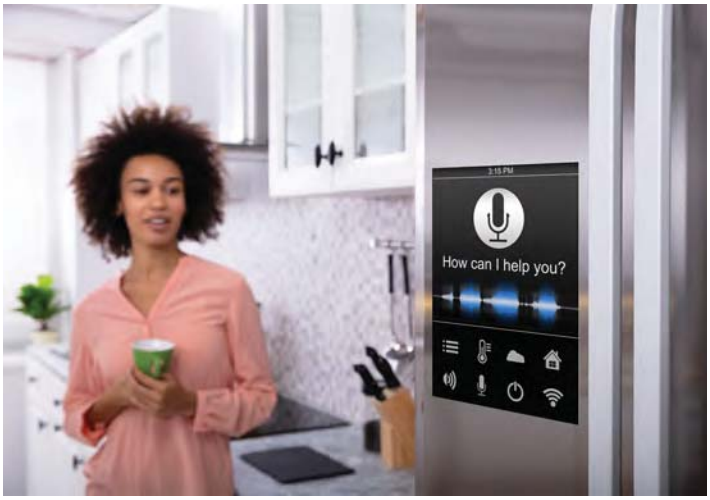
[7] KPMG research: **Includes** bills, standards and studies explicitly aimed at improving baseline security on IoT products and services. **Does not include** broader bills, standards and studies aimed at improving cybersecurity and/or consumer data privacy that may impact IoT device manufacturers but do not specifically focus on IoT security.

The writing is on the wall

Since IoT technology is evolving at a rapid pace, many of the current laws and proposals are purposely designed to be nebulous, allowing for flexibility down the road. But with so much evolving regulation—much of it incomprehensive, loosely defined, and open to interpretation—there is understandable confusion in the manufacturing industry about which aspects of which regulations apply to individual companies. How can manufacturers prepare to comply—or even know if they are at risk of being noncompliant—without an accurate picture of the regulatory landscape?

KPMG researchers did a deep dive into today's global regulatory environment, analyzing recent bills and those in the pipeline. Our analysis revealed eight core focal areas of the regulations.

The focal areas point to where the regulatory landscape is headed in the next few years and set the table stakes for what good future product security will look like. Many may sound straightforward. But the IoT is inherently complex. History shows that even leading-edge manufacturers sometimes fail to take basic steps to protect the end users of IoT devices: consumers. Evaluating the focal points of IoT security regulations will help manufacturing companies at any level of maturity understand where to prioritize investments in their device security program to ensure compliance and protect consumers.



The eight commonly identified thematic building blocks of sustainable IoT security regulatory compliance

Governance

Governance consists of organizational policies and processes to adequately address risk throughout the IoT lifecycle. It is the foundation underneath and engine that drives compliant connected device security programs and turns them into sustainable platforms. Product manufacturers must have effective governance in place to shape the direction of the program, enable collaboration among stakeholders, promote standardization and consistency, provide leading practices, and monitor regulatory risks on an ongoing basis.

Risk assessment

Risk assessment is a core component of governance and integral to the planning and strategy of effective IoT product security programs. To safely and effectively operate the business, manufacturers must understand the risks connected devices present to their own operations and assets as well as their key stakeholders, including consumers. A robust approach to risk assessment—which evaluates both immediate threats and potential threats that may emerge down the line—is the first step toward designing secure products, helping manufacturers understand where to focus security efforts.

Supply chain management

IoT device manufacturers are expected to authenticate and verify the security posture of third parties involved in their operations. This includes suppliers that play a part in designing, building, sourcing, and delivering product hardware materials and software components. It also includes suppliers integrated into other aspects of business operations, from the assembly line to the warehouse to the shipping port. Unique to the IoT device lifecycle, it also includes oversight of software vendors that continue to interact with devices after they leave the factory floor and are delivered into consumer hands.

Secure development lifecycle

IoT products should be designed end-to-end with security in mind—from prototyping to development to deployment. Manufacturers are expected to incorporate secure development lifecycle (SDL) techniques into the design and production of connected devices. SDL is an established, repeatable process for embedding security and risk mitigation into software at all layers of the technology stack. This includes embracing security and privacy by design principles, a technology development approach in which privacy and security requirements and architecture are integrated into the product during the early development stages. Security and risk validations cannot be late-cycle tollgates, but rather cultural principles sustained throughout the lifecycle. When applying SDL practices to IoT products, organizations stand to achieve real long-term cost savings and operational efficiencies.

Configuration management

The ability to customize preset software and firmware configuration is a key feature of many IoT products, enabling consumers to enhance the usability, privacy, and interoperability of the device after it is in their possession. This includes taking actions as simple as customizing a password or changing basic privacy settings to more complex actions, such as adding encryption to a device. However, the root causes of many IoT device incidents have been tied to weaknesses in the device's default settings or the ability to modify settings—intentionally or unintentionally—in a way that weakens their security. Manufacturers are responsible for ensuring secure default configurations that are preset into IoT devices. They are also responsible for controlling who can make changes to configurations and what kind of changes can be made.

Identity management authentication, and access control

Identity management, authentication, and access control ensure use of connected devices is limited to authorized people, processes, and devices. Manufacturers should embrace software security best practices for these areas, such as eliminating default passwords like "admin" that are easily exploitable, enabling each device to be uniquely identified, securely storing and transmitting sensitive data like usernames and passwords, restricting the number of access attempts allowed, thwarting improper attempts to gain unauthorized access, and minimizing exposed attack surfaces by closing unused ports and disabling unused services.

Data management and privacy

Manufacturers are responsible for implementing reasonable methods to protect data that is generated, collected, stored, and transmitted to connected devices. Only authorized access to, use of, and disclosure of data—each deemed appropriate to the function of the connected device—should be permitted. Manufacturers are also expected to ensure the availability, confidentiality, and integrity of data needed to deliver post market IoT services. Leading practices in secure data management and privacy include end-to-end encryption, secure storage mechanisms, the ability to wipe stored data, and clear and transparent data usage policies. Notably, effective data management and privacy approaches are not only necessary for manufacturers to build consumer trust, but also to mitigate regulatory risk. Consumer privacy protection is increasingly the focus of regulators, with far-reaching rules such as HIPAA, COPPA, the General Data Protection Regulation (GDPR), and the California Consumer Privacy Act (CCPA).

Vulnerability monitoring, management, patching, and response

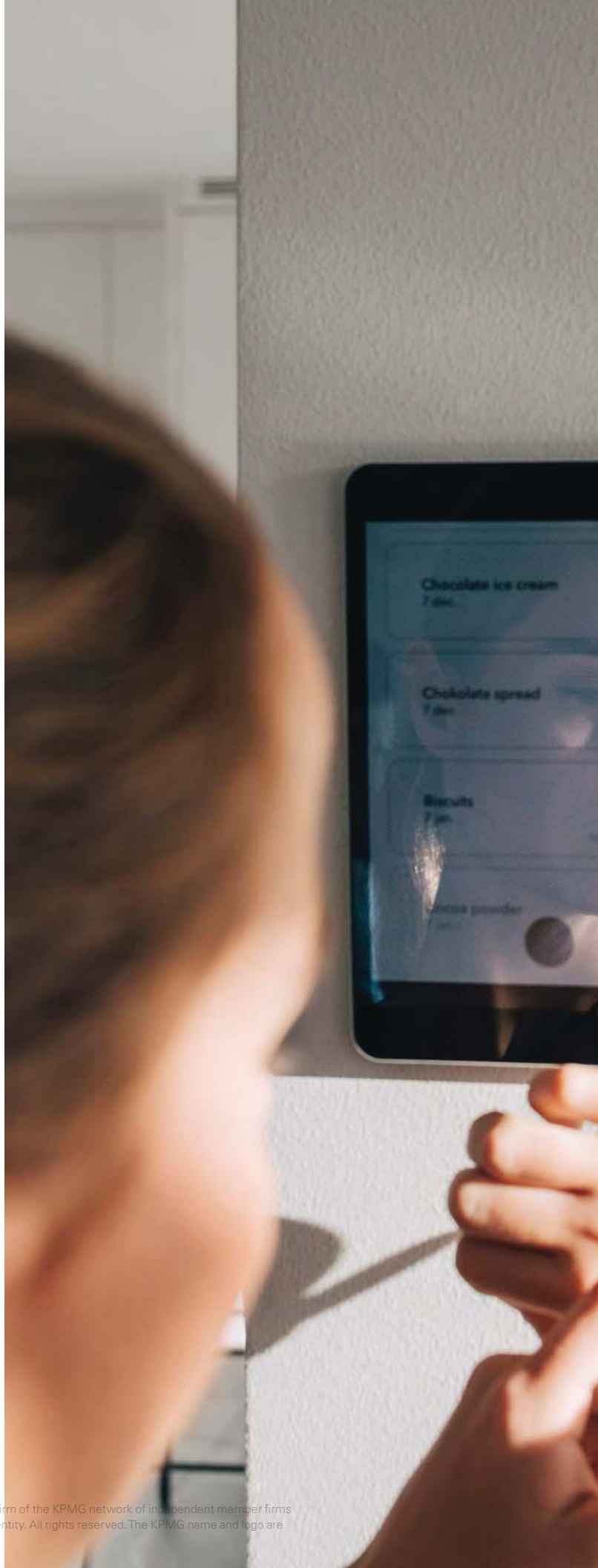
IoT product security doesn't end once a product is released. From malware to ransomware to eavesdropping, threats to software and hardware are evolving each day as malicious actors launch ever more sophisticated attacks. To mitigate risks as they arise, manufacturers are expected to actively and continually monitor, identify, and fix security problems in IoT devices, including those in production and in operation. Manufacturers should implement formal processes to monitor data for anomalies, detect intrusions in real time, discover security vulnerabilities (ranging from basic data monitoring to leading-edge methods like penetration testing and ethical hacking), update pre- and postmarket devices with security fixes, and disclose known vulnerabilities to affected stakeholders and the public at large.

Short-term compliance won't deliver long-term value

Perhaps the easiest and most obvious way for manufacturers to respond to the current regulatory push is to ready the organization to pursue simple compliance with the specific requirements that are applicable to the business today. But that is a shortsighted solution.

From a big picture standpoint, focusing on complying with IoT security rules on an individual basis is only applying a Band-Aid to the problem and may threaten manufacturers' customer relationships, profit potential, and market position if they aren't well-prepared for the future. The digital age is raising the stakes on trusted technology. In the connected world, technology has an unprecedented impact on customer experience and the level of trust customers place in manufacturers. Trusted technology is a key market differentiator, leading to stronger and more lucrative long-term relationships. Expertly designed, secure products win customer loyalty. Poorly designed, insecure products breach trust, send customers running, and seriously damage the manufacturer's brand. Therefore, doing the minimum when it comes to product security and privacy won't be enough to earn customer trust and use it to build competitive advantage.

In addition, approaching compliance as a "check-the-box" type exercise will cause organizations to be perpetually responding to new compliance demands. Manufacturers today typically sell products on a global scale. With the proliferation of online commerce and digitized supply chains, the majority make connected devices that are used by consumers throughout the United States, as well as many regions around the world. Working to comply with each relevant regulation individually is neither efficient nor cost effective. Even for smaller manufacturers that sell only into particular states, complying with local regulations alone and ignoring broader ones could cause problems down the road. When the manufacturer enters a new market or its customer bases shift, one-off compliance will inhibit the company's growth.



Transform product security for the connected world

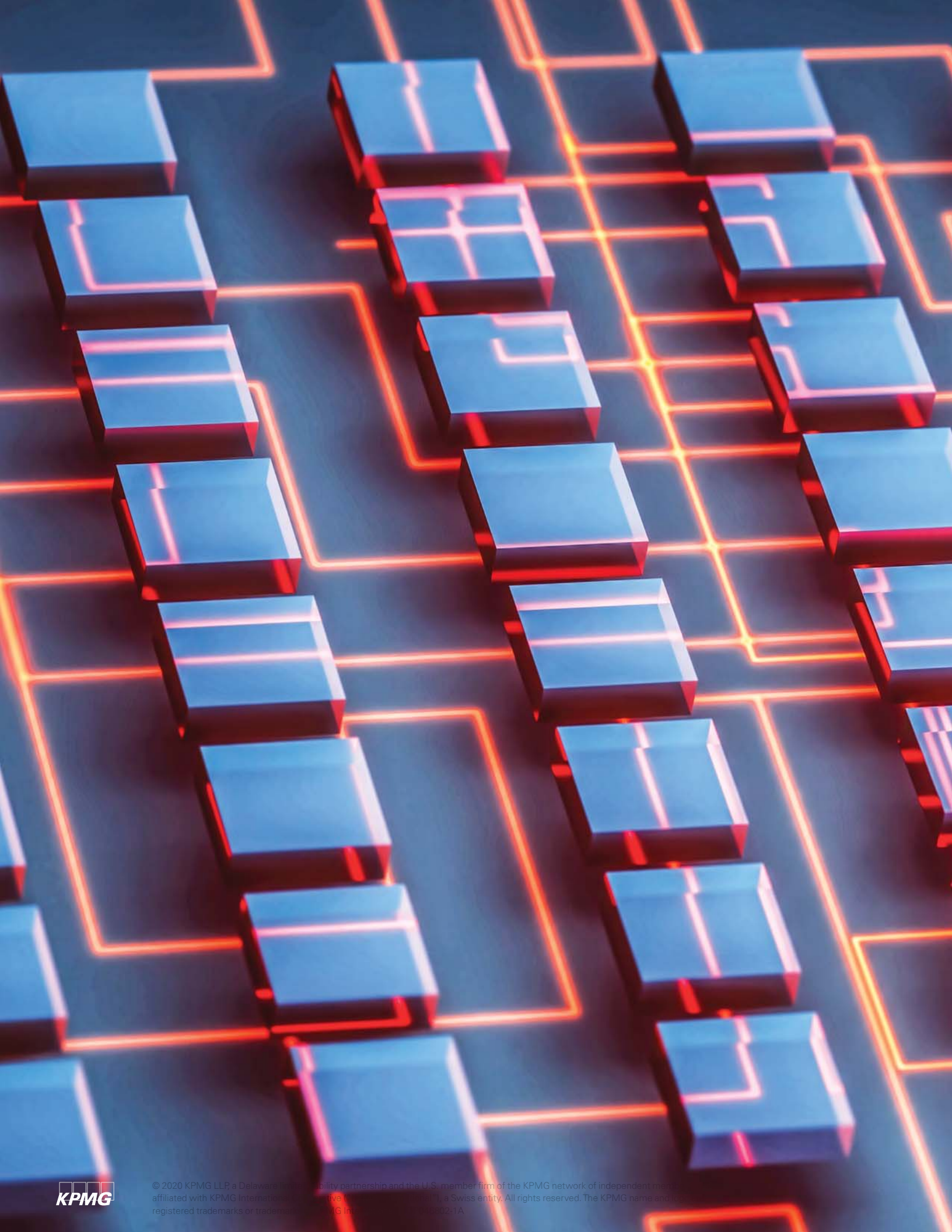
The wave of IoT security regulation shouldn't be just a compliance exercise. It should prompt manufacturers to do something they should already be doing: reinvent product security for the emergent IoT ecosystem.

The risks and complexities of the IoT are changing how manufacturers develop products and raising the stakes of security. Extra measures are needed to secure connected products from the factory floor to the owner's hand or home.

The financial reasons alone for improving product security are powerful. Without strong security and privacy in place, IoT manufacturers risk losing consumer trust, which is essential to earning their continued business. Now, as new IoT security regulations are enacted, the risk of running awry of rules and regulations should be added incentive for transformative change to security programs.

That's why the strategic response to the wave of IoT security regulations coming down the pike is to build and run a strong, robust, and sustainable product security program that is designed with consumer protection at the very center. Founded on best practices for trusted technology, an effective security program for internet-connected products embeds consumer protection into every element of the product lifecycle. A secure product provides a sustainable platform for customer adoption and growth.

A comprehensive and customer-focused product security program covers manufacturers' bases from a regulatory perspective, touching each of the eight focus areas of current regulations around the world. By reducing the risk of a technology incident, it also allows manufacturers to earn and preserve customer confidence in their connected products. And, it is capable of adapting to the passage of future laws: In today's ever-changing global regulatory landscape, that's essential for both business continuity and competitive advantage.



Product security blueprint for IoT manufacturers

Manufacturers will soon be forced to comply with a variety of new security rules and standards, with some having taken effect as early as January 1, 2020. Preparation must start immediately. But how should manufacturers get started?

We offer three initial considerations for manufacturers working to build best-in-class IoT security programs that achieve compliance with the regulations of today and tomorrow, all while earning consumer trust and enhancing the business value of IoT products and services.

— **Establish governance first:** An IoT security program is only as good as its governance. A strong governance foundation drives greater transparency and accountability for IoT risk management, allowing manufacturers to responsibly create, deliver, and support secure IoT products in the market—and comply with regulations, too. Risk assessment is a core piece of governance and should be an especially big focus of connected device makers. Risk assessment approaches like threat analysis and stress testing help companies understand the broad impact of security and privacy risks on product design, supply chain, consumer experience, and revenue streams. Good governance begins with the right people—including both business and technology stakeholders—collaborating to achieve shared strategic and operational goals, including IoT security regulatory compliance. Governance functions shape the overall direction of the IoT security program, drive consistency through process standardization, and promote security best practices throughout the IoT product lifecycle. There is no exact formula for the governance model: Some manufacturers operate a formal center of excellence while others draw resources from disparate groups working under a more decentralized approach. Manufacturing business and technology leaders should decide what works best within the constraints of their own organizational structures.

— **Prioritize traditional security best practices:** Compared to traditional consumer technology products, manufacturing safe and resilient internet-enabled devices requires enhanced security approaches and measures. But that doesn't mean the most important and fundamental principles of IT security and privacy are irrelevant. Rather, they remain the backbone for trusted IoT products. To protect consumers, security and privacy by design should be foundational elements of connected device development and production. Consistently applying traditional security best practices in related areas such as data management, identity management, and risk management will enable manufacturers to create a strong foundation for IoT device security. It will also set manufacturers on the path to regulatory compliance. As our analysis of IoT regulatory landscape revealed, expectations for baseline IoT security aren't drastically different than those for cybersecurity more generally.

— **Take a lifespan view of risks:** Once IoT products are deployed, manufacturers continue to send and receive valuable data to them, both to deliver services to consumers and to continually enhance the consumer experience. By building a trusted product, manufacturers entice consumers to continue to hand over their valuable data, which they can use to launch new services and open up new revenue-generating opportunities. In this way, the IoT ecosystem challenges manufacturers to ensure consumer safety even after products are no longer under their physical control. The ability of IoT product manufacturers to manage consumer security and privacy risks both pre- and post market is not only essential for consumer trust: It's also a key focus area of regulators around the world. In their view, manufacturers' responsibility for consumer safety only ends when IoT products are no longer functional nor connected to IoT networks. As such, manufacturers' processes for risk assessment, identity management, data management, vulnerability monitoring, incident response, and more must be comprehensive and continuous—yet also nimble, adapting to distinct and ever-evolving requirements for each stage of the IoT product lifecycle.

How KPMG can help

The IoT is expanding rapidly, creating tremendous opportunities in the consumer product space. At the same time, it's introducing new security and privacy risks to businesses and consumers.

KPMG's Emerging Technologies practice helps manufacturers generate value from IoT products by preparing business and technology functions to manage the unique risks of the IoT ecosystem. Our team is made up of talented technology specialists and risk management practitioners who specialize in helping manufacturers as well as companies in many other industries drive value from disruptive technologies like the IoT.

Drawing on our deep experience and forward-looking perspectives, we understand that only IoT products built on a foundation of security, resiliency, and trust will be able to meet evolving legal and industry standards designed to protect consumers. We work shoulder-to-shoulder with manufacturers from the ground up to responsibly develop, deliver, and support secure and compliant IoT products that stand out in a crowded market.

Strategy

— Establishing an IoT governance function and operating model

— Evaluating risk activities in the IoT program

— Developing tools and processes for continuous risk monitoring of connected devices

— Assisting management with defining their IoT risk and governance program roadmap

Delivery

— Defining and evaluating "security and privacy by design" principles

— Incorporating testing into the connected product quality assurance process

— Developing a connected device identification and classification schema

— Delivering training and awareness programs with common tools and enablers

Operations

— Monitoring and protecting connectivity, transmission, and storage of connected data

— Executing a formal data governance and data protection program

— Conducting ongoing vulnerability management and threat detection activities

— Managing, retaining, and analyzing data for continuous improvement and risk mitigation

Get in touch

Mike Krajecki
Managing Director, Emerging Technologies
KPMG LLP
T: 312-665-2919
E: mkrajecki@kpmg.com

Danny Le
Principal, Cyber Security Services
KPMG LLP
T: 213-430-2139
E: dqle@kpmg.com

Nick Naddaf
Manager, Emerging Technologies
KPMG LLP
T: 312-665-1594
E: nnaddaf@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia