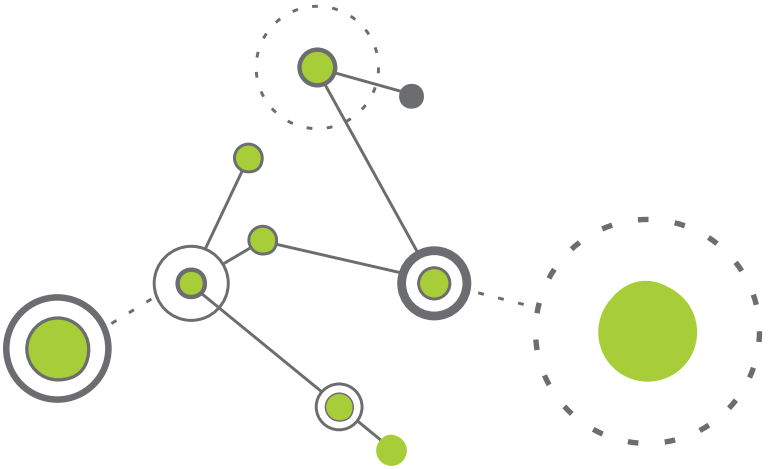
CAREFUL CONNECTIONS

Keeping the Internet of Things Secure



Federal Trade Commission | business.ftc.gov

Market analysts estimate that consumers and businesses around the world will use more than 20 billion Internet-connected devices by 2025. Internet of Things (IoT) companies design, manufacture, market, or support these connected devices – everything from light bulbs to smart TVs to wearable fitness trackers. As the industry has grown, so have the security risks. If a connected device is unsecure, it could give a hacker access not just to the confidential information transmitted by the device, but to everything else the device is connected to.

So, how should IoT companies think about security to protect people against these risks? There is no "one size fits all" approach to securing IoT devices, and what constitutes reasonable security will depend on a number of factors, including:

- the device functionality and purpose,
- the type and amount of information collected,
- the entities with whom the data is shared, and
- the level and likelihood of potential security risks involved.

To make sure your IoT company is taking reasonable steps to protect your customers' devices from hackers, thieves, and other bad actors, consider these recommendations from the FTC.

DESIGN SECURITY

When it comes to security, technology is ever changing, but certain time-tested principles remain.

- **Build security** into IoT product design from the beginning, rather than as an afterthought in the design process. Early in the development process, think through the data collected by the device, how people will likely use your product, and what features you can include to ensure security. What worked for your

first IoT device may be inadequate now. For example, consider the IoT ecosystem in which your device will operate. What, if any, other devices or systems will connect to your IoT device, and may use or share data from your device?

- **Stay aware of security** throughout the production process. Implement a **defense-in-depth approach** that incorporates security measures at multiple levels. Walk through how someone will interact with your product or service in a day-to-day setting to identify potential risks and possible security soft spots. If your IoT device offers password security, default passwords might sound like a good idea, but they quickly become widely known. Instead, think about using **unique passwords** and requiring consumers to change the password during set-up. Even better, offer **multifactor authentication** for stronger security. These steps, among others, such as using strong encryption and blocking access after a number of unsuccessful password attempts, can help guard against vulnerabilities like brute force attacks where hackers use automatic programs until they're successful at guessing a password.

- **Take a risk-based approach.** Unsure how to allocate your security resources? Conduct a risk assessment, taking into account the purpose, nature and functionality of your products and services. That will help you develop, implement, and maintain a security program that addresses the magnitude and severity of the risks identified. Free risk management frameworks are available from groups like the Computer Security Resource Center of the National Institute of Standards and Technology, or you may want to seek expert guidance.

- **Test security measures throughout development and again before launch.** It might seem obvious, but it's critical to conduct thorough testing of your product's security features before you put a connected device into the hands of the public.

USE RECOGNIZED SECURITY PRACTICES

Security experts have identified solutions to some common concerns raised by IoT. To guide your security practices, look at industry best practices and at lessons learned from law enforcement actions. Here are a few suggestions.

- Take reasonable steps to **address well-known and easily preventable security flaws**. Expert groups provide information that may help you implement appropriate safeguards and stay up to date on the latest security vulnerabilities. For example, security experts have long warned against threats like cross-site scripting attacks, where malicious scripts are injected into otherwise trusted websites, and cross-site request forgery attacks, where unauthorized commands are sent from a user the website trusts. Unless you take appropriate defensive measures up front, IoT devices may create unnoticed pathways into otherwise secure networks or may be used in a denial of service attack on another target.
- Implement strong **encryption techniques** that are available for the type of data your device transmits and stores. Encrypt sensitive data and consider well-known methods to make it harder for attackers to compromise data, such as applying multifactor authentication to secure your own systems.
- Make sure you understand and comply with **applicable standards, rules, and regulations**. For example, if you manufacture or market IoT devices for children, you may need to check out FTC guidance on the Children's Online Privacy Protection Rule. If your IoT device is health-related, you may be covered by the FTC Act, the FTC's Health Breach Notification Rule, the Department of Health and Human Services' Health Insurance Portability and Accountability Act (HIPAA), or the Food and Drug Administration's Federal Food, Drug & Cosmetic Act (FD&C Act). Don't forget about state legislation. California and Oregon enacted IoT laws,

effective January 2020, mandating stronger security safeguards for IoT devices.

Consider these other resources:

- National Institute for Standards and Technology Interagency or Internal Report NISTIR 8259 Foundational Cybersecurity Activities for IoT Device Manufacturers (csrc.nist.gov/publications/detail/nistir/8259/final)
- National Institute for Standards and Technology Interagency or Internal Report NISTIR 8259A IoT Device Cybersecurity Capability Core Baseline (csrc.nist.gov/publications/detail/nistir/8259a/final)
- Resources from the Open Web Application Security Project (OWASP), including:
  - OWASP IoT Top 10 vulnerabilities (owasp.org/www-pdf-archive/OWASP-IoT-Top-10-2018-final.pdf)
  - The OWASP IoT Security Verification Standard (ISVS) provides security requirements for IoT applications (github.com/OWASP IoT-Security-Verification-Standard-ISVS)
- Email updates or RSS feeds from trusted security sources. Check out free databases of vulnerabilities identified by vendors and security researchers regularly – for example, the National Vulnerability Database (nvd.nist.gov/).

AUTHENTICATE AND CONTROL ACCESS

Design your product with authentication in mind. This is another part of building security from the beginning. It's worth taking time early on to think through security, especially in key areas like authentication and access controls, rather than having to fix vulnerabilities later, once your IoT device is already in the hands of your customers.

- Implement **effective authentication protocols** for your device, data, and system, including stored and transmitted data. If a device transmits or receives sensitive data, an authentication failure could allow unauthorized access to that information and expose sensitive data stored on the device as well as on networks it's connected to. In addition, it could lead to unauthorized use of the device, which could allow a hacker to make harmful changes to the device settings and cause other problems. Strong authentication procedures help ensure that only authorized users can access the device, including its settings and its data. This includes, for example, considering multifactor authentication. It's important to test authentication techniques before release and periodically thereafter.
- **Secure remote access** to your networks and cloud servers. Implement adequate measures to segment and protect live systems from testing environments. You may even want to consider investing additional resources in the design, implementation, and testing of authentication and access controls. And use WPA2 or WPA3 – forms of encryption designed to protect wifi networks.
- Put **sensible access limits** in place, such as limiting administrative permissions, to keep unauthorized people from accessing IoT devices, data, or the network. Think about who needs access to the different areas in your system. For example, not every employee or vendor needs access to customers' sensitive data.

IMPLEMENT SECURE DATA MANAGEMENT

Consider a holistic approach to address the entire life cycle of data collection, transmission, storage, access, use, and, ultimately, secure data deletion associated with your IoT product or service. This includes working across different parts of your company (e.g., developers, security, and

marketing), and with third-party providers, to understand each group's data needs and to reinforce proper data management and security at all levels.

- Apply sound **data minimization** practices, such as limiting the collection of personal data, and retaining that information only for an essential period, not indefinitely. Think through the implications of your data management steps. Understand why you're collecting the data you collect, think through how and why you store or share data, and what you will do with it once you don't need it. Simply put: Don't collect, store, or share data that you don't need. If the data is necessary for the functioning of your product or service, be sure to communicate that to users, and take reasonable steps to secure that information, both in storage and during transmission. You could also choose to take steps like de-identifying data once collected.
- Perform **timely security reviews**, including vulnerability and penetration testing, as applicable to new uses, upgrades, new connection capabilities and other types of changes. Based on a risk assessment, protect the interfaces between your product and other devices or services. A security weakness at the contact point where a service communicates with your device could give scammers a foothold into your network. That's why each of those interfaces needs to be secured and monitored. Periodically revisit how you are using and protecting data.
- Properly **segment your network** and monitor who's trying to get in and out. Would you know if an intruder was attempting to grab data or hijack IoT devices on your network? There are tools that can alert you when someone is trying to transfer large amounts of data, and when they are using devices in appropriately.

MONITOR AND ADDRESS SECURITY RISKS

Security is a dynamic process, and can benefit from the cross-talk that goes on among technology experts, researchers, and your customers. Some recent law enforcement actions have cited companies' failure to follow up when credible sources warned them about security vulnerabilities in their products. That's why it's wise to take advantage of the expertise that's already out there and listen to what people are saying.

What else can you do?

- Implement a process to **actively monitor and address security** vulnerabilities, and perform security tests, such as maintaining intrusion detection and data leak prevention systems. In particular, check for vulnerabilities in third-party components that are integrated into your products. Securing your software and networks isn't a one-and-done deal. It's an ongoing process that requires you to monitor vigilantly. Check for both expected and unexpected behaviors. For example, make sure that the transmitted data is encrypted and that it's the data that should be transmitted.
- Pay attention to **credible security warnings**, investigate, and move quickly to fix them. When security concerns prove to be accurate, reach out to customers immediately.
- Consider providing automatic **security patches** to cover known risks. IoT device users are often unaware of updates, particularly when the only way to find an update is for them to actively search the manufacturer's website. Automatic updates to address known vulnerabilities will reduce the risk of people using unsupported IoT devices. And when providing updates, ensure that the process is reasonably secure.

- Take sensible steps to **address threats** to privacy, security, and safety before and after launch. Maintain an adequate process for receiving and addressing security vulnerability reports from security researchers and academics. Consider establishing a bug bounty program to encourage reports of discovered vulnerabilities and other problems.

Create a culture of security. Encourage a culture of security within your company and share your security attitude with others, like third-party vendors or service providers. For example, designate a senior executive who will be responsible for product security. In addition, ensure downstream privacy and data protections through vendor contracts and oversight.

- Set **clear security expectations** for employees. Train your employees periodically on good security practices, including how to recognize the latest threats and vulnerabilities. Because some people in your organization may be less familiar with technology and security, design your training to be effective for those individuals. Your training should be different for IT security professionals versus marketing professionals, for example.
- Provide **regular security and privacy training** to your device engineers, and send frequent security and privacy reminders to help prevent them from falling victim to social engineering tactics, such as targeted phishing attempts. When successful, phishing attempts could allow cybercrooks to access your customers' devices – for example, as a result of your engineers giving out admin passwords.
- Agree on **third-party security practices**. If you work with service providers, make sure they are capable of maintaining, and actually maintain, reasonable security. Incorporate security standards into your contracts (e.g., providers should adopt reasonable security precautions such as encryption). And take

reasonable steps to verify compliance with those security standards on an ongoing basis. For example, if you require your service providers to commit not to re-identify the data, monitor them to make sure they live up to their promises.

COMMUNICATE

Proper and clear communication from the start may save you – and your customers – the substantial costs of a security incident.

- Strive to be **simple, clear, and direct** in your communications about security. Using generic names and descriptions may confuse your customers. Don't use complicated jargon or hard-to-find hyperlinks on your website. If you collect customer data, be transparent. Explain the data collected, along with how and why you are collecting it and how you intend to secure the data. Remember that your customers may have different levels of technical expertise, so it's important to craft your communications accordingly. Provide an easy way for your customers to contact you with their questions and concerns.
- Consider **pre-purchase disclosures** about functionality and support. When people buy IoT devices, they generally expect that the things they buy will work and keep working, and that security controls have been established as a default. These expectations include any technical or other support necessary for essential functioning. If privacy and security will not be protected throughout the life of a product, truthfully convey that. They should know the extent to which you intend to provide security updates for your devices, and how the updates will be made. Would users expect the device's security to have an "expiration date"? Or would they expect to be able to keep using a fully functional device indefinitely?

- **Innovate how you communicate** with users. Some IoT devices may not even have a screen, so manufacturers should consider helping people sign up for notifications about security support either at the point of sale or after. Keep security separate from marketing communications, which might deter your customers from agreeing to receive such information.
- **Don't wait** to notify customers when security issues arise. Think through how you'll let them know about fixes. With security issues, time is not usually on your side – especially when security issues require not only your action, but action on the part of your customers, too. Say someone spots a problem and you design a patch to address it. That's an important first step, but the job's not done. A security patch is effective only if customers install it. So make sure that you build a contingency plan to address the challenges of notifying your customers after the sale about fixes and patches, and how to apply them.

Want more?

- Cybersecurity for Small Business (ftc.gov/tips-advice/business-center/small-businesses/cybersecurity)
- Start with Security: A Guide for Business (ftc.gov/tips-advice/business-center/guidance/start-security-guide-business)
- NIST Cybersecurity IoT Program, National Institute for Standards and Technology (NIST) (nist.gov/programs-projects/nist-cybersecurity-iot-program)
- Securing the Internet of Things, Department of Homeland Security (dhs.gov/securingtheIoT)

About the FTC

The FTC works for the consumer to prevent fraudulent, deceptive, and unfair practices in the marketplace. The Business Center gives you and your business tools to understand and comply with the law. Regardless of the size of your organization or the industry you're in, knowing – and fulfilling – your compliance responsibilities is smart, sound business. Visit the Business Center at **business.ftc.gov**

Opportunity to Comment

The National Small Business Ombudsman and 10 Regional Fairness Boards collect comments from small businesses about federal compliance and enforcement activities. Each year, the Ombudsman evaluates the conduct of these activities and rates each agency's responsiveness to small businesses. Small businesses can comment to the Ombudsman without fear of reprisal. To comment, call toll-free 1-888-REGFAIR (1-888-734-3247) or go to **sba.gov/ombudsman.**

Federal Trade Commission
business.ftc.gov
September 2020