Buying IoT Technology: How to Contract Securely

By Nicholas R. Merker, Partner, Ice Miller LLP

More and more products are shipping with sensors and network connectivity to capitalize on the currency of data. Data interconnectivity between these devices creates new opportunities to identify and support insights about how use of these products impacts your company. For example, a meeting room may automatically turn on its lights and air conditioning ten minutes before a scheduled meeting by using third-party software; your employees may transmit data about how many steps they've taken, their heart rate and their caloric intake to a third-party vendor as part of a wellness program; and equipment all throughout the enterprise (from the trash can to the HVAC system) might generate alerts to third-party vendors when in need of repair.

What happens when your network-capable trash can becomes the entry point for a hacker?

What do you do when your wellness vendor is compromised and employee data is published on the internet? How do you know your Internet of Things ("IoT") products are safe?

These are not academic questions. The 2013 Target Corp. data breach reportedly stemmed from a compromise of network credentials maintained by a third-party HVAC vendor.[1] Recent research also reveals how old cybersecurity vulnerabilities are present in new network-capable, consumer-facing products, like baby monitors.[2]

In the United States, costs associated with data breaches have risen each year over the last three years.[3] When a breach of consumer or proprietary business information occurs, a company will pay costs for audit and consulting services, legal services for defense and legal services for compliance.[4] A company that negotiates information security into its contracts to purchase third-party IoT products may avoid some of these costs, either through risk transfer or by avoiding the incident completely. Of course, identifying and mitigating cybersecurity risks with these vendors requires collaboration among multiple business units and a vendor willing to negotiate.

This article will discuss how a lawyer may address risk management during the contract negotiation process. It is broken down into two phases of the procurement process: product evaluation and contract negotiation.

Product Evaluation

The product evaluation phase in IoT procurement is critical. A lawyer cannot intelligently negotiate a procurement contract without understanding how the network-capable product is going to be utilized in the environment and/or whether a third-party vendor will require access to the product (e.g., for maintenance). Take one example — if your company is purchasing a surveillance camera that is equipped to generate an alert when it detects sound, the risk associated with installation of that camera is much different depending on where it is deployed logically and physically, who has access to the data it generates and what features are enabled or disabled. In this example, if the camera is deployed above the water cooler and is accessible by the third-party vendor to conduct maintenance, you may have concerns over the privacy of employee conversations that could be captured by the camera. If, however, the camera is deployed over an external door at a remote site, that concern is nonexistent. In another

example, if the camera is deployed in the United States, the privacy and data security risks are much different than if the camera is deployed in the European Union.

Understanding how the product is deployed, what information it will collect and how that information will be used will require conversations with those at your company who will be using and maintaining the product, including information technology, privacy, and information security. Although these conversations may naturally happen through your company's vendor management practices, one way to kick-start them is to implement privacy-by-design. Privacy-by-design is an approach to protecting privacy by embedding it into the design specifications of technologies, business practices, and physical infrastructures.[5] A key tenet of privacy-by-design is to think about privacy in the design and architecture of systems and processes at the outset. A company that implements privacy-by-design would require that company stakeholders discuss how the implementation of a new IoT product would impact privacy and information security for the organization.

Once a company understands how an IoT product will work in its environment, the next step in product evaluation is to understand how that product alters the company's risk profile through a risk assessment. A risk assessment is the process of identifying risk, assessing risk, and taking steps to reduce risks to acceptable levels for the organization.[6] How your company conducts a risk assessment may be determined based on your industry, the type of information you collect, how your company is regulated, or by industry standard. There are many different risk assessment strategies and guidance available and entire articles could be written on this concept alone.[7]

Many risks identified in this process will be mitigated without the involvement of legal, possibly through network design, identity and access management, disabling unnecessary features or implementation of other security safeguards. Some unacceptable risks, however, might be ripe for mitigation through contract.

Contract Negotiation

With an understanding of the risks that need to be mitigated through contract, a lawyer is equipped to enter negotiations. The following list of key contractual terms may be helpful during this process. Of course, as discussed above, not all of these terms may be material — your deployment of the IoT product will dictate which terms you need to spend your negotiation capital on to make sure your contract aligns with your risk mitigation strategy.

Establish and Maintain an Information Security Program

Require an IoT vendor to establish, implement and maintain an information security program which requires the vendor to maintain commercially reasonable security safeguards designed to protect against any unauthorized or illegal access, loss, destruction, or other exploitation of the purchased IoT product. A strong information security program at the IoT vendor will help ensure that your company's data gathered by the IoT product and sent back to the IoT vendor will not be misused, either by the company or an unauthorized third party.

What is "commercially reasonable" will vary dramatically based on your industry and the compliance regime that you must follow. It is also somewhat difficult to understand what constitutes commercially

reasonable information security for any business. It is much easier to say what is clearly not commercially reasonable than it is to say what is commercially reasonable. For example, the Federal Trade Commission has stated that storing passwords in clear text is not commercially reasonable.[8]

In an attempt to make the concept of commercially reasonable more understandable, you can cite to industry guidelines. The FTC has produced an IoT cybersecurity guide for businesses, the U.S. Food and Drug Administration has established a set of guidelines for IoT cybersecurity in medical devices, and other industry groups are attempting to establish frameworks for IoT cybersecurity.[9]

Another way to make the concept of commercially reasonable more understandable is to align the vendor with your information security expectations by enumerating the types of cybersecurity safeguards that you expect will be implemented. For example, you can specify that the vendor implement a strong asset management program, establish a strong termination procedure to prevent former employees from accessing your company data, implement reasonable physical security controls at data centers, and require encryption of your company data at rest and in transit.

IoT product procurement also may require additional considerations by the vendor regarding how the product was developed. Consider requiring that the vendor represent and warrant that it has developed the product using reasonable information security coding practices, such as by requiring its developers to undergo secure code training, establishing peer code reviews, performing penetration testing and quality assurance of its IoT product before deployment into the market and others.

Cybersecurity Incident Response

In the unfortunate event that your IoT product directly or the third-party vendor who receives data from it or has access to it is compromised, you do not want to be left holding the bag for losses resulting from that breach. As discussed above, the cost of remediation efforts (e.g., legal defense, forensics, etc.) resulting from a data breach is high, and you may negotiate that your IoT vendor covers these costs. Given the high cost associated with a data breach, also consider that you require your IoT vendor to procure cyber-risk insurance that will apply when a data breach occurs related to the IoT product.

Additionally, your IoT vendor may be in a better position to know that a security incident has occurred. For example, if they receive alerts from the IoT device or routinely log in to the IoT device for maintenance purposes, your vendor may know that an attacker has gained access to the device and pulled data from it before you do. Consider requiring that your IoT vendor notify you immediately in the event that it learns of a security incident. With some laws requiring notification to consumers impacted by a breach within 30 days, you want your vendor to notify you much sooner than that to give you time to evaluate the incident and plan a response.

Jurisdictional Compliance

Depending on your industry and the location you deploy your IoT product, you may have jurisdictional requirements that you want to ensure are met. For example, if your IoT product is collecting personal data of data subjects in the European Union and transferring that data to a United States entity for processing, you will want to ensure that the IoT product conforms to the European Union's strict requirements for processing personal data and for transferring that personal data out of its jurisdictional

borders. Similarly, if your IoT product might collect government data in the United States, you will want to ensure that data does not leave the country.

Downstream Obligations

Another key risk that is ripe for mitigation in the contracting process is addressing how your IoT vendor utilizes its own third-party service providers. If your IoT vendor engages a subcontractor for any purpose, make sure to require that this subcontractor conform to the same information security requirements that you expect of the IoT vendor itself.

A quick example highlights the importance of this requirement. In 2015, the Indiana attorney general entered into a settlement with a local dentist who was accused of mishandling records containing sensitive patient information. The attorney general alleged that the dentist hired a private company to retrieve and dispose of old patient records, but the third party simply discarded the records in an Indianapolis dumpster rather than appropriately disposing of them.[10]

Audit Rights

Requiring that your vendor comply with all of these information security requirements via the contract is a great step in mitigating risk. However, a contract is merely an instrument and does not guarantee compliance. To verify that your vendor is adhering to these requirements, consider negotiating an audit provision that gives you or your third-party independent auditor the right to enter the vendor's premises and conduct an assessment. This assessment may be a strict review of your vendor's compliance with its contractual obligations or a review of your vendor's adherence to an accepted set of industry standards. Alternatively, rather than conducting an audit yourself which might be at your cost, you may consider requiring that the vendor undergo an audit from an independent third party and produce the results of that audit to you on an annual basis.

Conclusion

This article is not meant to be exhaustive of the contractual terms that you will want to negotiate during IoT procurement. It aims to identify some key terms that you may not have considered material in these types of negotiations. It should be appreciated, however, that an attorney negotiating a contract for IoT product procurement should understand how that product will be deployed in your company to truly appreciate the risks that need to be mitigated.

For more information on the Internet of Things and its liabilities, contact Nick Merker or a member of our Internet of Things practice group.

[1] Target Hackers Broke in Via HVAC Company, Krebs on Security (Feb. 5, 2014).

[2] Mark Stanislav and Tod Beardsley, HACKING IoT: A Case Study on Baby Monitor Exposures and Vulnerabilities, Rapid7 (September 2015) (identifying backdoor credentials, direct browsing,

authentication bypass, and predictable information leak vulnerabilities in certain baby monitors); J.M. Porup, "Internet of Things" security is hilariously broken and getting worse, Arstechnica (Jan. 23, 2016).

[3] Ponemon Institute, 2015 Cost of Data Breach Study: Global Analysis (May 2015) (costs rising from $188/record in FY2013 to $217/record in FY2015).

[4] Id.

[5] Information and Privacy Commissioner of Ontario, Introduction to PbD.

[6] Technology Administration, U.S. Department of Commerce, Special Publication 800-30 Rev. 1, Risk Management Guide for Information Technology Systems, National Institute of Standards and Technology, p. 1.

[7] See, e.g., Technology Administration, U.S. Department of Commerce, Special Publication 800-30 Rev. 1, Risk Management Guide for Information Technology Systems, National Institute of Standards and Technology; U.S. Department of Health & Human Services, Final Guidance on Risk Analysis; PCI Security Standards Council, Information Supplement: PCI DSS Risk Assessment Guidelines.

[8] Federal Trade Commission, RockYou Inc. Enforcement.

[9] Federal Trade Commission, Careful Connections: Building Security in the Internet of Things; U.S. Food and Drug Administration, Cybersecurity; UL, Product Testing and Validation.

[10] American Dental Association, Indiana dentist is first sued by state for violating HIPAA (Mar. 2, 2015).