The Computer & Internet Lawyer

Volume 38 ▲ Number 3 ▲ March 2021

Ronald L. Johnston, Arnold & Porter, Editor-in-Chief

Managing Vendor Cybersecurity Risk in IoT Contracting

By Linda L. Rhodes, Marcus A. Christian, and Charles King III

Use of IoT[1] devices continues to grow exponentially as companies leverage the impressive data collection abilities of technology to drive exciting developments.[2] It is estimated that by 2025, there will be over 64 billion IoT devices in use worldwide.[3] Expansion is further fueled by the remote working environment arising out of the COVID-19 pandemic. Necessitated out of stay-at-home orders and social distancing requirements, vast numbers of workers whose jobs revolve around digital communication devices are logging into systems, and interacting with colleagues and clients, from their homes or other remote locations. As the infrastructure for remote working is implemented and improved, the chances of a return to the pre-COVID-19 status quo becomes less likely.

The expansion of connectivity presents growing security risks and challenges for companies across a wide range of business sectors. For example, companies engaged in the manufacture of consumer products typically embed into their products, and/or develop solutions relying on the interaction with, the technologies of one or more vendors. In enterprise IT, companies rely on third-party technology vendors, which in many cases access the companies' systems and/or hold the companies' data on the their systems. In the new world of remote workforces, companies need to be concerned with not only the security of their vendors' systems but also the security of remote environments from which vendor personnel may be working.

In an increasingly connected world, cybersecurity vulnerabilities are amplified as additional end points provide threat actors with more means to reach critical systems through more sophisticated and varied attacks, resulting in a range of harms such as business interruptions, financial loss, and even personal injury. Further, businesses also face unique cyber threats and security

Linda L. Rhodes, a partner in the Washington, D.C., office of Mayer Brown LLP, has over 30 years of experience representing clients on complex commercial transactions, with a primary focus on technology transactions. **Marcus A. Christian**, a partner in the firm's Washington, D.C., office, represents clients in matters involving data security planning, board governance of cybersecurity, cyber fraud, data breach response, and congressional investigations, among other matters. **Charles King III**, an associate in the firm's Chicago office, focuses his practice on business process outsourcing, data center leasing, and technology transactions related to cloud services and software licensing. The authors may be contacted at *lrhodes@mayerbrown.com*, *mchristian@mayerbrown.com*, and *charlieking@mayerbrown.com*, respectively.

challenges presented by the COVID-19 pandemic given that remote work environments are unlikely to maintain the same level of security safeguards as are maintained in work facilities.[4]

Vendors play a key role in cybersecurity. This article explores the criticality of managing vendor cybersecurity risk as a cornerstone of a company's cybersecurity program.

Current Legal Landscape

Given the upside of innovative technology, and the significant repercussions of security breaches, a lot of thought has gone into how to mitigate cybersecurity risks associated with connected devices. Lawmakers have weighed in through legislative efforts, and the resulting legislation reflects a clear understanding of the need to protect connected devices and manage vendor cybersecurity.

While federal IoT legislation has been proposed in the United States, the U.S. federal government has yet to pass any of it into law. However, California has stepped up to start filling the gap. It recently became the first state to implement an IoT-specific law, which took effect on January 1, 2020. California requires manufacturers of connected devices to equip such devices with a "reasonable security feature."[5] The "reasonable security feature or features" must be (i) appropriate to the nature and function of the device; (ii) appropriate to the information it may collect, contain, or transmit; and (iii) designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure.[6]

The EU Cybersecurity Act, which became effective in June 2019, takes a somewhat different approach by focusing on certification for ICT (information and communications technology) products, services and processes sold in the European Union, yet the purpose is essentially the same – to make ICT devices safer and more secure in recognition that security and resilience are not yet sufficiently built into products, services and processes.

States have enacted laws to ensure management of vendors when it comes to cybersecurity and data privacy. For example, Massachusetts, a leader in data breach notification law, requires companies to "take reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect . . . personal information consistent with these regulations and any applicable federal regulations."[7] Massachusetts further requires companies to "[require] third-party service providers by contract to implement and maintain such appropriate security measures for personal information. . . ."[8]

Industry laws and regulations, such as the Gramm-Leach-Bliley Act, Department of Transportation National Highway Traffic Safety Administration ("NHTSA") safety regulations and automated vehicle technologies guidance, the Food and Drug Administration rules and regulations, and many others, directly and indirectly through their safety and protection regulations, approvals, and/or recall authority, impose their own requirements around connected products and must be taken into account in a company's approach to, and contracting for, cybersecurity. Federal agencies such as the Department of Homeland Security and the Department of Commerce have provided guidance on how to manage the security of connected devices, and the Federal Trade Commission ("FTC") has asserted its authority to bring enforcement actions for "unreasonable" IoT cybersecurity practices.

Recommendations for Contracting

"Reasonable Security Features"

California's new IoT law requires that connected devices have "reasonable security feature(s)." The FTC has asserted its authority over "unreasonable" IoT cybersecurity practices. Under Massachusetts law, companies are required to cause third-party service providers to implement and maintain "appropriate security measures." But what do "reasonable" and "appropriate" really mean? If businesses continue to operate under "work from home" policies due to the pandemic, will that affect which security features qualify as "reasonable" and "appropriate"?

The California law provides some guidance on what constitutes a "reasonable" security feature(s). First, the security feature(s) must be appropriate to the "nature and function of the device" and the "information it may collect, contain, or transmit." Therefore, for example, a connected device that collects personal entertainment preferences in order to provide entertainment value may require different security features than a device that collects and transmits financial data to accomplish financial transactions or that collects and transfers personal health information to monitor and/or treat health issues. The California law further requires that the "reasonable security feature(s)" be designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure. These principles not only need to apply to the company's components and technologies but must be extrapolated to its vendors in order for the company to meet security obligations applicable to it and, in some cases, legal mandates to pass through such security obligations. Failure to do

so can result in regulatory violations, as shown by the FTC's willingness to bring claims against device manufacturers that fail to exercise proper oversight over their service providers.[9]

Vendor contracts often include a covenant for the vendor to implement and maintain reasonable, appropriate, and adequate security measures and safeguards – after all, many cybersecurity and privacy laws require it. However, should a security incident arise and regulators and plaintiffs ask you to demonstrate that security features (including those provided by your vendors) were in fact reasonable, appropriate, and adequate, pointing to a single sentence in a contract is not a winning strategy. From a contractual perspective, an agreement that goes further in requiring that the security and safeguards be sufficient for compliance with laws and compliance with applicable industry standards, such as those published by the International Organization for Standardization ("ISO"), the International Electrotechnical Commission ("IEC"), and the National Institute of Standards and Technology ("NIST"), reflects a deeper understanding of the complexity of cybersecurity risk management.

Exercising due diligence and performing risk assessments is critical for determining whether connected devices are equipped with reasonable and appropriate security features. Possibly, the hardest part of due diligence is knowing what to ask. Among the many items that may be included on a vendor due diligence "checklist," cybersecurity diligence is key. What is the function of the vendor's technology and what information does it collect, contain and transmit? What protective features have been designed into the device technologies? The first step is to actually ask the vendor those very questions and then to have conversations and request documents and other information to support the answers. In order for the vendor's component or technology to work, what connections to other critical components of the device are required? This is not a simple question nor one the vendor is likely to be able to answer alone; rather, the company may be in the best position to analyze technology interconnections, but surely information from its vendors will be required in the process for a comprehensive analysis. Managing vendor cybersecurity risks requires mapping out data flows among all the parties – the end user, the company and the vendor or multiple vendors – as well as required connectivity, with an understanding and balance of the need for interconnectedness to provide desired features and functions vs. the need for separation and isolation where possible and necessary for the protection of the cybersecurity of critical systems.

As noted above, "security by design" is an important and pervasive concept in cybersecurity. But how will a company know that its vendor components and technologies were designed with security in mind, in particular if the company is acquiring or licensing from a vendor technology that predates or is developed outside of the contractual relationship? Again, a good first step is to ask the question, and follow that up with further diligence. Depending on the nature of the technology and its purpose or use, security questionnaires and audits may be needed to fully assess the security design features. Many companies, in particular those in regulated industries, already face regulations and guidelines imposing "by design" obligations such as "safety by design" and "privacy by design." "Cybersecurity by design" is yet another layer of due diligence investigation.

California now imposes an obligation on companies to ensure "security by design." These questions are no longer relevant to only AV technologies, medical devices and the like, but are principles to be applied across all connected devices. Many vendor contracts include representations and warranties that vendor products and work product comply with documented specifications but consider whether to expand those representations and warranties to state that such products and work product were, and will be, designed with security in mind.

What Is Your Contract Missing?

How will your company demonstrate that that contractual requirements have been adhered to? Are your audit rights sufficient to allow you to access the people, process and information you need to ensure compliance throughout the term and in case a cybersecurity incident arises? For example, where a claim arises under the new California IoT law, you may need to demonstrate that a technology embedded in a connected device was designed with cybersecurity in mind. A right to audit contractual compliance may not extend to design information unless you've thought to put in related contractual obligations.

Who needs the right to audit – the company and its auditors for sure, but what about cybersecurity experts engaged by the company to help with the investigation of a security incent? If a security incident occurs – or is even suspected or threatened – you may engage a third-party cybersecurity expert to conduct the audit. Yet, the information discovered by such a third party may be discoverable in the event of an investigation or litigation. The results of the audit may reveal information on vulnerabilities or failures to protect against threats that should have been known to the company. Accordingly, you may want the flexibility for your legal counsel to

engage auditors so that the audit results will be protected by legal privilege.

How long do the audit rights last? An enterprise IT vendor contract may permit the company to audit a vendor during the term of the agreement and a tail period thereafter, but is that sufficient in a contract for connected technologies that may be embedded in devices used by the company's customers long after the contractual relationship expires?

Similarly, a company likely has ongoing responsibilities to provide technology security patches to customers of connected devices post-sale. Accordingly, the relationship of the customer and vendor often must continue well after the product is sold. Therefore, ongoing maintenance and technology fixes are important aspects to consider when contracting for connected device components and services. Vendor contracts should clearly define maintenance requirements and ensure that connected devices will be supported over time.

Conclusion

The contracting recommendations described in this article are by no means exhaustive but are intended to provide context and considerations for companies in managing vendor cybersecurity risk. In order to build a comprehensive cybersecurity contracting strategy, companies need to understand the legal landscape and manage vendor risk from the beginning of the design process through the lifecycle of connected devices.

Notes

1. "The internet of things, or 'IoT,' is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction." Margaret Rouse, Internet of Things (IoT), *IoT Agenda* (retrieved Aug. 14, 2020), *available at https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT*.
2. Econsultancy, 10 Examples of Internet of Things in Healthcare (Feb. 1, 2019), *available at https://econsultancy.com/internet-of-things-healthcare/*; IoT for All, How IoT is Driving the Autonomous Vehicle Revolution (June 8, 2018), *available at https://www.iotforall.com/iot-and-autonomous-vehicles/*.
3. Christo Petrov, 47 Stunning Internet of Things Statistics 2020 [The Rise of IoT], TechJury (Aug. 2, 2020), *available at https://techjury.net/blog/internet-of-things-statistics/#gref*.
4. One way that cyber criminals are exploiting these opportunities is through phishing attacks, which have seen a 350 percent increase during the pandemic. Jason Cohen, Phishing Attacks Increase 350 Percent Amid COVID-19 Quarantine, PCMag (Mar. 30, 2020), *available at https://www.pcmag.com/news/phishing-attacks-increase-350-percent-amid-covid-19-quarantine*.
5. S.B. 327, 2017-2018 Reg. Sess., (Cal. 2018), *available at https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB327*.
6. Similarly, the new NY SHIELD Act requires companies to "develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity" of the personal data, and Ohio provides an "affirmative defense" for a data breach if a company has a cybersecurity program that complies with certain requirements. S.B. S5575B, 2019-2020 Reg. Sess., (New York 2019), *available at https://www.nysenate.gov/legislation/bills/2019/s5575*; S.B. 220, 132nd Gen. Assembly, (Ohio 2018), *available at https://www.legislature.ohio.gov/legislation/legislation-summary?id=GA132-SB-220*.
7. 201 CMR 17: M.G.L. c. 93H, (Mass.), *available at https://www.mass.gov/doc/201-cmr-17-standards-for-the-protection-of-personal-information-of-residents-of-the/download*. Similarly, the New York DFS requires companies to perform "periodic assessment of . . . Third Party Service Providers based on the risk they present and the continued adequacy of their cybersecurity practices. . . ." 23 CRR-NY 500.11 (New York), *available at https://govt.westlaw.com/nycrr/Document/I60c644470d5f11e79781d30ba488e782?viewType=FullText&originationContext=documenttoc&transitionType=CategoryPageItem&contextData=(sc.Default)*. The GDPR requires that a controller must only use processors "providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject." EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/49, *available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679*.
8. 201 CMR 17: M.G.L. c. 93H, (Mass.), *available at https://www.mass.gov/doc/201-cmr-17-standards-for-the-protection-of-personal-information-of-residents-of-the/download*. Similarly, the EU GDPR requires a controller to include in its contract with a processor that the processor "take[] all measures required pursuant to [the security provision of the GDPR]." EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/49, *available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679*.
9. BLU Products, FTC No. 1723025 (April 30, 2018) (complaint), *available at https://www.ftc.gov/enforcement/cases-proceedings/172-3025/blu-products-samuel-ohev-zion-matter*.