



CYBER ALERT ■

DECEMBER 20, 2019

Preparing for the CCPA: Reasonable Security – Can You Produce It?

By [*Kim Peretti*](#), [*Amy Mushahwar*](#) and [*Kate Hanniford*](#)

A company's information security program may satisfy baseline notions of reasonable security (and may even be technically innovative), but how does it demonstrate reasonable technology deployment, staffing, and processes when faced with scrutiny from regulators, allegations by plaintiffs, or inquiries from business partners? As the California Consumer Privacy Act (CCPA) compliance deadline nears and regulatory scrutiny continues to intensify, the need to demonstrate successful implementation of reasonable security requirements has never been more critical. The trend for regulators and business partners to make increasingly voluminous requests of companies and to expect responses—including supporting documentation—within tight deadlines has highlighted the need for in-house counsel to proactively evaluate (1) the extent to which a company's information security program is reasonable and defensible; and (2) how it can show that reasonable security is in place using typically generated artifacts of compliance.

To evaluate both the reasonableness of current state security and the strength of evidence to demonstrate that security, a holistic approach with participation from and coordination across legal, information security, information technology, and other operational divisions is necessary. Moreover, the exercise of identifying and demonstrating artifacts of compliance is an effective means to verify that the contemplated controls that underpin a company's reasonable security are in fact in place. This allows stakeholders to have further confidence in the state of security for the organization.

Evaluation of Reasonable Security

Although companies in the financial, payment card, health care, energy, and telecommunications sectors have been subject to more scrutiny of their security programs for many years, it is hard to overstate the transformation of the reasonable security landscape as a result of recent changes to state law requiring companies to implement and maintain reasonable security, often through a written information security program, as codified in New York, Massachusetts, Oregon, and Nevada statutes, for example. More than half of all U.S. jurisdictions have enacted laws requiring reasonable security measures, although their application may vary based on type of business and/or information collected.

This advisory is published by Alston & Bird LLP to provide a summary of significant developments to our clients and friends. It is intended to be informational and does not constitute legal advice regarding any specific situation. This material may also be considered attorney advertising under court rules of certain jurisdictions.

In addition to the evolving expectations for reasonable security that are applied to companies through the patchwork of federal and state laws, the looming compliance deadline for the CCPA as well as the private right of action enshrined in that law has the potential to further intensify scrutiny of information security programs across industry sectors. Currently, a company that experiences a significant breach may be subject to (1) regulator oversight in the form of federal sector-specific requirements, congressional inquiry, state attorneys general investigation, and even city-level investigation; and (2) consumer, investor, and business-partner claims. The CCPA adds another element of litigation risk because under the CCPA, the failure to implement reasonable security becomes actionable following a data security breach. More specifically, the CCPA presents a watershed moment for consideration of what exactly constitutes reasonable security and how one shows it in such a way that minimizes the nature, scope, and duration of a regulator investigation or discovery.

Although the CCPA contains an (untested) 30-day period to “cure” a breach before consumer suits, Ohio remains the only U.S. jurisdiction with a safe harbor grounded in reasonable security and available to companies defending against tort claims brought in Ohio or under Ohio law as a result of a data breach. But because the Ohio safe harbor does not apply to contract claims, which can frequently arise from data security incidents, its practical use may be limited. At a time when the overall incidence and costs of data security incidents are increasing year-over-year, the need to be prepared to demonstrate reasonable security has never been more compelling.

Generally, both federal and state statutes and regulations that require reasonable security of a covered company hinge on the development, implementation, and maintenance of administrative, physical, and technical safeguards—requiring an examination of people and company culture, in addition to technical deployments. Although the specific safeguards necessarily vary based on the company’s risk profile, they derive from the company’s risk assessment as well as its data and asset inventories. From a regulator perspective, it is commonly expected that a company’s information security program should be able to meet or exceed the threshold for reasonable security since the concept of reasonable security is well-established and the tools needed to establish and maintain that security have become more widely available and scalable for a company’s given risk profile.

Yet flexibility in the wording of the law and the variety of the mechanisms available to support security also pose risks to companies because industry standards and evolving cybersecurity threats may be more easily recognized in hindsight. One strategy to mitigate this risk is for an information security program to formally adhere to widely recognized third-party security frameworks, such as NIST’s SP 800-171, SP 800-53, or SP 800-53A; FedRAMP; COBIT; the CIS Critical Security Controls; or the ISO 27000 family. In addition, entities in the health or financial sector may benchmark their information security programs to the cybersecurity frameworks articulated in HIPAA, GLBA, FISMA, or HITRUST, as appropriate. Similarly, entities subject to the PCI Data Security Standard (PCI DSS) may formalize language and practices in their written information security program that mimic PCI DSS to safeguard cardholder data. Companies can also use industry standard reporting mechanisms for service provider oversight, such as the Standardized Information Gathering Questionnaire (SIG), helpful tools for assessing the baseline security environment of a third party.

However, a company's effort to achieve reasonable security can be exacerbated by the fact that it is subject to overlapping regulatory and audit requirements. In such circumstances, a legal assessment or gap analysis is often the most efficient means to align a company's chosen information security framework with the regulatory requirements to which a company is subject. The analysis then can be used to test and assess whether the information security program complies with identified requirements and standards in practice. That is, a company should be able to verify that its information security practices and controls as reflected in its stated policies, procedures, ticketing, logging, and technical dashboards meet or exceed the regulatory requirements as well as the industry standards the company uses to benchmark its compliance. Companies may find that engaging outside counsel to perform this gap analysis and direct the technical assessment of information security practices and controls under privilege is an effective and prudent way to identify and close potential compliance gaps before a regulator or private plaintiff has a chance to pick apart a company's state of compliance.

Demonstration of Reasonable Security

Although it is widely accepted that companies must establish reasonable security, how does a company produce it? The challenge for many companies lies in moving beyond the assessment of reasonable security to being able to document and produce artifacts that in the aggregate show reasonable security to an outside third party. Companies can take additional proactive steps to get ahead of the curve and be well-positioned to respond to regulator requests in a timely fashion, and this work should ideally take place before a third-party request is on the horizon. Beginning with a coordinated effort, personnel from legal, information security, information technology, and other appropriate business lines should gather potentially responsive, core documents and/or dashboarding ahead of time. A company can then build a working set of the governance documents and supporting artifacts of compliance that are likely to be requested and the company should consider when preparing its submissions to regulators and business partners, including narrative responses. For each security domain, it may be useful for a company to consider the presence or absence of certain artifacts of compliance.

- **Program Governance.** In addition to the written information security program itself, companies should anticipate regulator requests for board minutes or briefings and the cybersecurity budget and personnel information relating to the information security and information technology teams, including team list, background, and training information. This information can be relevant to assess the relative expertise and size of the program, as well as the context of investigations involving insider threats.
- **Risk Assessments.** The most recent risk assessment and the results of any other security audit, review, or assessment over the past year should be collected and organized. This would include internal audit report recommendations, identified deficiencies, and status of remediation items (including the company risk register or POAMs). Third-party certifications and representations, assessments, or findings associated with those certification and renewal exercises would also be potentially in scope for those that are not conducted under the attorney-client privilege.

- **Baseline Evidence.** Evidence of compliance and corrective actions can include screenshots (or a WebEx walk-through procedure) that demonstrate the effective implementation of particular tools as well as reports or other automatically generated reports and analysis. Compiling such reports can serve as representative examples of the effectiveness of network and event monitoring tools, for example, as well as proper IT ticket and event handling.
- **Key Risk Areas.** More specific documentation may also be gathered according to key risk areas or based on the company's assessment of its threat landscape. For example, policies, procedures, controls, standards, and artifacts of compliance relating specifically to (1) network and systems architecture; (2) access controls; (3) change management/project management; (4) disaster recovery; (5) patch and vulnerability management; and (6) vendor risk management are six common high-risk areas that should also be anticipated.
 - **Network and Systems Architecture.** Regulators or business partners may request systems and network maps, which may provide context for their inquiry.
 - **Access Controls.** Beginning with controls such as password management, multifactor authentication, IP whitelisting, and/or geo-blocking, a company may want to gather a range of artifacts as simple as screenshots, user training materials, and user acknowledgements to show a broad and sustained commitment to access controls. In addition, representative examples of more sophisticated SIEM monitoring and log analysis that would show the enforcement of such access controls can be beneficial.
 - **Change Management/Project Management.** Depending on the risks associated with the development and deployment of software, a company may need to closely manage this area. Artifacts of compliance can include ticketing, technical reports, or the fulfillment of other preset milestones as reported in periodic scrums, screenshots of beta testing, or other quality assurance before launch.
 - **Disaster Recovery.** A company could compile documentation showing recent verification of regularly scheduled data backups as well as tests of backup communications systems, warm sites, and other mechanisms identified in the business continuity/disaster recovery plans that are critical to resiliency.
 - **Patch and Vulnerability Management.** Evidence of reasonable security can include screenshots showing adherence to regularly scheduled patch schedules, successful application and testing of patched applications, and ad hoc patches applied based on manufacturer instructions and recommended timing. The most recent results of periodic penetration testing and any internal or external scanning activities can also be helpful to compile.
 - **Vendor Risk Management.** Given the prevalence of vendor incidents, it may be beneficial to gather material vendor contracts and associated compliance policies in addition to evidence of third-party service provider oversight activities, including timelines for regularly scheduled vendor assessments. Artifacts of service provider oversight can include completed questionnaires, security audit reports, penetration testing, industry vendor documentation (e.g., BitSight and Security Scorecard), and documents supporting corrective actions in response to those questionnaires or reports.

To maintain the core set of reasonable security documentation once gathered, it is critical for the company to secure them and to limit access to only those users who have a legitimate need. In addition, companies may find it useful to periodically update the file with current documentation, particularly as any identified gaps are closed or enhanced measures are implemented. As a result of this effort, once the company has actually received a request, it will be able to focus on crafting its message instead of scrambling to compile documents.



In addition to the efficiency gained during the regulatory response period, a primary benefit of collecting and organizing key artifacts of compliance with reasonable security requirements is that it affords the company the chance to uncover areas of noncompliance or divergences from stated policies and procedures in time to correct the course before regulator scrutiny. By identifying potential pain points early in the process, a company may have time to address them unprompted by regulator or plaintiff attention.

The cross-department coordination required to ensure and demonstrate regulatory compliance may not come easy for a company. If a company can initiate that coordination early and without the time pressure of a regulatory deadline, it may be easier for the working group to hold key discussions, review evidence of compliance together, and ensure that the various departments understand the current state of security. This includes reaching a common understanding of the significance and nuance to certain artifacts of compliance and how they may or may not fulfill regulatory expectations either in isolation or in combination with one another. This process facilitates a company's ability to respond more accurately and transparently to a regulator and to provide requested information quickly and clearly.

Cybersecurity Preparedness & Response Team Co-Chairs

Kimberly Kiefer Peretti | 202.239.3720 | kimberly.peretti@alston.com

Jim Harvey | 404.881.7328 | jim.harvey@alston.com

Follow us:  @AlstonPrivacy |  www.AlstonPrivacy.com

www.alstonsecurity.com

ALSTON & BIRD

WWW.ALSTON.COM

© ALSTON & BIRD LLP 2019

ATLANTA: One Atlantic Center ■ 1201 West Peachtree Street ■ Atlanta, Georgia, USA, 30309-3424 ■ 404.881.7000 ■ Fax: 404.881.7777
 BEIJING: Hanwei Plaza West Wing ■ Suite 21B2 ■ No. 7 Guanghua Road ■ Chaoyang District ■ Beijing, 100004 CN ■ +86 10 8592 7500
 BRUSSELS: Level 20 Bastion Tower ■ Place du Champ de Mars ■ B-1050 Brussels, BE ■ +32 2 550 3700 ■ Fax: +32 2 550 3719
 CHARLOTTE: Bank of America Plaza ■ 101 South Tryon Street ■ Suite 4000 ■ Charlotte, North Carolina, USA, 28280-4000 ■ 704.444.1000 ■ Fax: 704.444.1111
 DALLAS: Chase Tower ■ 2200 Ross Avenue ■ Suite 2300 ■ Dallas, TX 75201 ■ 214.922.3400 ■ Fax: 214.922.3899
 LONDON: 5th Floor, Octagon Point, St. Paul's ■ 5 Cheapside ■ London, EC2V 6AA, UK ■ +44.0.20.3823.2225
 LOS ANGELES: 333 South Hope Street ■ 16th Floor ■ Los Angeles, California, USA, 90071-3004 ■ 213.576.1000 ■ Fax: 213.576.1100
 NEW YORK: 90 Park Avenue ■ 15th Floor ■ New York, New York, USA, 10016-1387 ■ 212.210.9400 ■ Fax: 212.210.9444
 RALEIGH: 555 Fayetteville Street ■ Suite 600 ■ Raleigh, North Carolina, USA, 27601-3034 ■ 919.862.2200 ■ Fax: 919.862.2260
 SAN FRANCISCO: 560 Mission Street ■ Suite 2100 ■ San Francisco, California, USA, 94105-0912 ■ 415.243.1000 ■ Fax: 415.243.1001
 SILICON VALLEY: 950 Page Mill Road ■ Palo Alto, California USA, 94304-1012 ■ 650.838.2000 ■ Fax: 650.838.2001
 WASHINGTON, DC: The Atlantic Building ■ 950 F Street, NW ■ Washington, DC, USA, 20004-1404 ■ 202.239.3300 ■ Fax: 202.239.3333