DORSEY
DORSEY+WHITNEY LLP

CCPA Requires "Reasonable Security": but You Can't have Reasonable Security Without Proper Vulnerability Management

September 16, 2019 – Dorsey Health Law
by Divya Gupta and Cody Wamsley

The Dorsey Health Law blog team keeps readers up-to-date on relevant topics in the health care industry. In order to do so, the members of the blog team communicate regularly with other practice groups within the firm for applicable updates from client publications. For this post, we would like to thank Dorsey's Divya Gupta and Cody Wamsley for the following e-news letter update:

With the California Consumer Privacy Act ("CCPA") set to take effect on January 1, 2020, and the resulting looming specter of statutory damages and data breach class action litigation for failure to implement "reasonable security" on the near horizon, reducing or mitigating the harms that result from such cyber-attacks is more important than ever. Since 2015, more than three in five Californians have been a victim of a data breach, making implementation of reasonable security controls now a critical and necessary component of CCPA compliance.[1] While the retail industry has had record breaking breaches from malware and hacking, especially with card data, no industry is risk free when it comes to adequate data security.

Managing or mitigating risk, however, requires implementing "reasonable security," which derives from the Center for Internet Security's Top 20 Critical Security Controls (CSC 20) per then California Attorney General in 2016, Kamala Harris. In California's 2016 Data Breach Report, Harris stated that "[The CSC 20] are the priority actions that should be taken as the starting point of a comprehensive program to provide reasonable security."[2] Recommendation 1 of the same report is more explicit:

The 20 controls in the Center for Internet Security's Critical Security Controls identify a minimum level of information security that all organizations that collect or maintain personal information should meet.

The failure to implement all the Controls that apply to an organization's environment constitutes a lack of reasonable security. (emphasis added).

Based on these statements, the CSC 20 likely comprise a defensive list to detect,

Related Capabilities

- Healthcare & Life Sciences
- Healthcare Transactions & Regulations
- Healthcare Litigation
- Medical Devices

prevent, respond to, and mitigate security incidents, and are designed to address various domains of information security to provide organizations with a roadmap to achieve resiliency. Whether the CSC 20 will become the explicit standard for "reasonable security" is still an open question, but given the California AG's previous statements, these controls should be top-of-mind for any organization that seeks to avoid significant liability under the CCPA.

The CSC 20 is broken down into three main categories of controls: Basic, Foundational, and Organizational. The total scope of the CSC 20 is beyond the scope of this article, but suffice it to say that an organization may be hard-pressed to assert that it has "reasonable security" in place if it does not at least adhere to the Basic controls. The Basic controls consist of the following 6 items:

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

Of these 6 Basic controls, #3, Continuous Vulnerability Management, stands out as one of the most important for an organization to focus on to prevent data breaches. According to a recent study, nearly 60% of recent data breaches were the result of unpatched vulnerabilities.[3] Indeed, the California AG stated that "patching newly discovered security vulnerabilities is critical" while citing the related CSC 20 control. In the last few years, the importance of vulnerability management has become more apparent and this control has risen to become the #3 control in the CSC 20.

Vulnerability management's main purpose is to identify and remedy software vulnerabilities as quickly as possible. It often doesn't take any significant skill on an attacker's part to exploit published vulnerabilities and so once a software vendor releases a patch, knowledge of its associated vulnerability quickly becomes widespread and the race is on between organizations deploying patches and attackers attempting to exploit the vulnerability. Organizations that do not scan for and proactively address vulnerabilities are at great risk for a breach.

Patching software security is a no-brainer, or so you'd think. Well, the challenge lies in the scale of the organization, the effect a patch could have on other organization systems, and the attacker's ability to quickly weaponize ahead of scheduled patch rollouts, among other things. To properly implement vulnerability management may not be as easy as we'd like, but it is critical and low-hanging fruit on the CSC 20 tree.

The European Union deems privacy a fundamental human right, and is taking enforcement seriously -- think Marriott and British Airways GDPR fines. We expect to see similar, if not greater, liability for organizations that violate the upcoming CCPA. Organizations that haven't yet automated the process to monitor for and remediate

vulnerabilities on networks and systems should do so now and should institute vulnerability and patch management policies. While all of the CSC 20 controls are important, perhaps the most effective solution to prevent a major data breach for any organization lies in assessing and managing known vulnerabilities. Modernizing vulnerability management programs should be a focus in the short term run up to January 1, 2020 effective date.

Dorsey's Cybersecurity and Privacy Team has developed a catalog of security practices and procedures to help achieve operational resilience and defend companies from the forthcoming wave of data breach litigation. Notably, Dorsey has partnered with leading technical security industry organizations to offer full service advice.[4]

Additional references:
https://www.us-cert.gov/sites/default/files/c3vp/crr_resources_guides/CRR_Resource_Guide-VM.pdf
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf
https://www.sans.org/reading-room/whitepapers/threats/implementing-vulnerability-management-process-34180

[1] See California's 2016 Data Breach Report, available at https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf.
[2] https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf.
[3] https://www.darkreading.com/vulnerabilities---threats/unpatched-vulnerabilities-the-source-of-most-data-breaches/d/d-id/1331465.
[4] https://www.dorsey.com/services/cybersecurity-privacy-social-media.