CALIFORNIA ATTORNEY GENERAL SETS NEW MINIMUM STANDARD OF CARE FOR DATA PRIVACY & SECURITY

Batya Forsyth, William Kellermann and Everett Monroe Hanson Bridgett LLP

INTRODUCTION

California is long recognized as at the forefront with the development of computer technology in all its forms. California took the lead with legislation to protect its citizens from identity theft and other cybercrimes when it enacted the first statutory definition of personally identifiable information and the first data breach notification law.

Nevertheless, with the exception of certain regulated industries, the Federal Trade Commission (FTC) has led in enforcing and encouraging good data security practices nationwide. Widely recognized as the top privacy cop in the United States, it approached data security as a consumer protection issue under its authority to prosecute unfair and deceptive practices. It has published documents discussing good data security practices, and has used its enforcement authority to obtain consent decrees requiring companies to implement comprehensive data security programs.

As more data breaches at major institutions garner national attention, states have been developing and increasing their role in enforcing data security laws, and have started providing or adopting guidelines that reflect their enforcement priorities, their missions, and their scope of authority.

Not to be left behind, and as a major recipient of data breach notifications, the California attorney general adopted a set of standards known as the *Critical Security Controls* (CSC) as minimum requirements to comply with California law. The CSC set a floor by which to evaluate the duty of care to which businesses who hold data of California residents will be held.

This article examines some of those motivations and compares the set of controls adopted by California's top law enforcement agency with other standards that have guided businesses in establishing their data security programs.

CALIFORNIA'S NEW STANDARD OF CARE

California law, along with a number of other states, requires that businesses maintain reasonable security to protect their customers' personal information. But the technologically neutral term, meant to reflect the "reasonableness" standard of tort law, does not define reasonable security.

The California attorney general, who has the authority to enforce the data security law, issued its most recent biennial Data Breach Report in February 2016. The report recommended that all companies should implement the Center for Internet Security's *Critical Security Controls.* More importantly, the recommendation expressed the attorney general's view that a failure to implement the CSC would be a failure to implement reasonable security procedures that California law requires.

The CSC are published by the Center for Internet Security (CIS) of the SANS Institute, and were developed as a collaborative effort by data security professionals. The CSC are numbered in order of priority: the first control is the most important to establish, the second control next, and so on. Each control includes sub-controls that companies can evaluate as potentially beneficial security measures. While the sub-controls suggest specific tasks that a business could take to implement the control, the CSC do not prescribe any particular practices.

The CSC provide detailed and technical descriptions of tasks to undertake compared to other standards that use broader, more procedural language. Given its data security expert origins, the CSC focus more on protecting data and networks on a technical level, with fewer controls addressing administrative measures for data security.

Many of the CSC come from the same industry wisdom around which other security frameworks and standards were created. Businesses that developed data security programs around other guidance and frameworks may find that they need to add or change little to fully implement the CSC.

COMPARING & CONTRASTING STANDARDS – THE NIST FRAMEWORK

The adoption of CSC and the increased regulation around data security provides an incentive for businesses to start building a data security program. But the CSC, while thorough, can be complex. Through the CSC, CIS does not provide much guidance on establishing and administering a data security program. For those starting out on the path to robust cybersecurity, other frameworks and guidance might be a better place to start.

In particular, the National Institute of Standards and Technology (NIST) published the Framework for Improving Critical Infrastructure Cybersecurity. The Framework provides step-by-step instructions for a company to create, develop, and assess a data security program in an organization of any size.

The Framework organizes a data security program into a set of five functions: Identify, Protect, Detect, Respond, and Recover. Each function contains a set of categories that a business should evaluate to determining its level of maturity in incorporating each function. Taken together, the functions move businesses through the process of protecting data from establishing a program to addressing data breaches.

Many of the CSC can be met through implementing the Framework. Many of the CSC controls are reflected in the Protect and Detect Functions. The Framework's thorough guidance in its Respond and Recover Functions corresponds to Control 19: Incident Response and Management. Once a program is on its way to development, a business can use the CSC to strengthen its technological controls in the Protect and Detect Functions.

A business that has built their cybersecurity program can then use the CSC to fill in certain gaps, come into compliance, or further mature their programs. But the CSC includes additional requirements not found in the Framework. The Framework would probably view Control 15: Wireless Access Control and Control 20: Penetration Tests and Red Team Exercises as a highly advanced implementation not necessary for all businesses.

HOW THE CSC COMPARE WITH THE FTC DATA SECURITY REQUIREMENTS

California companies that approach data security as a compliance issue typically look to guidance from the FTC. As one of the few legally enforceable standards, The FTC's data security guidance comes from a combination of enforcement actions and publications on best practices. The FTC's guidance, as an agency whose data security enforcement comes from its authority to protect consumers and their personal information, takes a broader, less technologically detailed approach than the CSC.

The most comprehensive document issued by the FTC, Protecting Personal Information: A Guide for Business, organizes its data security framework into five steps, each containing a number of tips and actions that businesses can implement. The guidance takes a more data-focused approach, placing an emphasis on limiting the collection of personal information to what is necessary for business use and protecting it. The FTC also provides specific guidance for technology that might go unnoticed, such as digital copiers, and incorporates federal legal requirements focused more on privacy than security.

Protecting Personal Information does not provide the same robust guidance of the CSC, and in many circumstances would only partially implement the CSC. For example, the FTC's guidance on password management and employee training barely touches on the appropriate use of administrator access to computer systems, which the CSC prioritize as a means of preventing unauthorized use of credentials.

For businesses who have been complying with the FTC that want to or need to comply with the CSC, the focus should be on implementing practices that are important to good data security, but may not be directly related to protecting the unauthorized use or disclosure of personal information. In particular, ensuring that your company can ensure data recovery in the event of a loss of access due to ransomware, and making sure that configurations for wireless access and network devices are properly secured to prevent unauthorized access should be priorities.

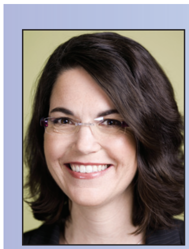
ADDING INTERNATIONAL FLAVOR: THE ISO STANDARDS

Companies that have a global footprint or have a need for a more universally recognized set of standards may be guided by publications from the International Organization for Standardization (ISO). ISO is an international body made up of the national standards setting bodies of 162 countries that issues standards on a wide range of topics. ISO standards 27001 and 27002 on data security have been widely adopted in the U.S. and globally, and are more comprehensive than the NIST Framework.

The ISO standards focus on data security from a management perspective. Most of the CSC are focused on a mere few of the ISO Standards. Properly implemented, an ISO compliant system of data security should cover all the CSC, though the technological implementations may not be as robust as focusing on the CSC exclusively. A company may be well served by following the ISO standards as a practical matter, but it may not be as useful when coming under the particular scrutiny of any given regulator.

CONCLUSION

Regardless of the standards that a company selects, there are common steps any business can take to establish or build their data security program. For businesses starting on the path, they should evaluate the framework best suited to their business needs and determine how they can best invest resources in providing better data security. Businesses should also make sure to adequately document their data security programs and be prepared to demonstrate compliance with the standards, should a state or federal agency come to call. Finally, businesses should view data security as a process – as the threats change, their data security practices will need to respond to the changes in risk.



Batya Forsyth is a partner at Hanson Bridgett and the co-chair of the firm's Privacy, Data Security and Information Governance practice. She is a Certified Information Privacy Professional/United States (CIPP/US). Batya's litigation practice includes bank customer disputes related to secured and unsecured loan products, deposit accounts and collections and business disputes on behalf of owners, licensors, and service providers related to breach of contract, fiduciary duty and fraud.

William Kellermann is Electronic Discovery & IG Counsel at Hanson Bridgett. William helps clients execute sound and defensible identification, preservation, collection, review and production of electronically stored information for use as evidence in litigation and investigations. In addition, he assists enterprises with litigation readiness and information governance counseling focused on defensible retention and disposition programs, and structured legal hold and litigation response systems for pattern litigants.

Everett Monroe is an attorney at Hanson Bridgett. He focuses on data privacy and intellectual property disputes and counseling, two areas in which his technical background as an electrical engineer join with his legal experience to serve clients in a range of complex matters. Everett is a Certified Information Privacy Professional/U.S. Government (CIPP/G) and a Certified Information Privacy Professional/Europe (CIPP/E).