Kroll | A Division of DUFF & PHELPS

Morgan Lewis

Potential Pitfalls of the CCPA Exemptions

Ensuring Reasonable Security Implementation

Nov 2019

Today's Discussion

MODERATOR

Jonathan Fairtlough

Managing Director,
Cyber Risk, Kroll

PANELISTS

Reece Hirsch

Co-head, Privacy &
Cybersecurity Practice,
Morgan Lewis

Keith Novak

Associate Managing Director,
Cyber Risk, Kroll

Cole Manaster

Senior Associate,
Cyber Risk, Kroll

Agenda

1. Reasonable Security
2. CCPA vs GLBA vs HIPAA
3. Key Takeaways

Reasonable Security

CCPA **Requires** Reasonable Security

- A lack of reasonable security is a prerequisite to the private right of action for security breaches
- Under proposed CCPA regulations:
  - Reasonable security measures required when transmitting personal information in response to a consumer's request to know or delete
  - Reasonable security measures required to detect fraudulent identity verification activity and prevent unauthorized access or deletion

What Constitutes Reasonable Security

The 20 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**.

California Data Breach Report (Feb 2016) Attorney Gen. Kamala D. Harris

Reasonable Security

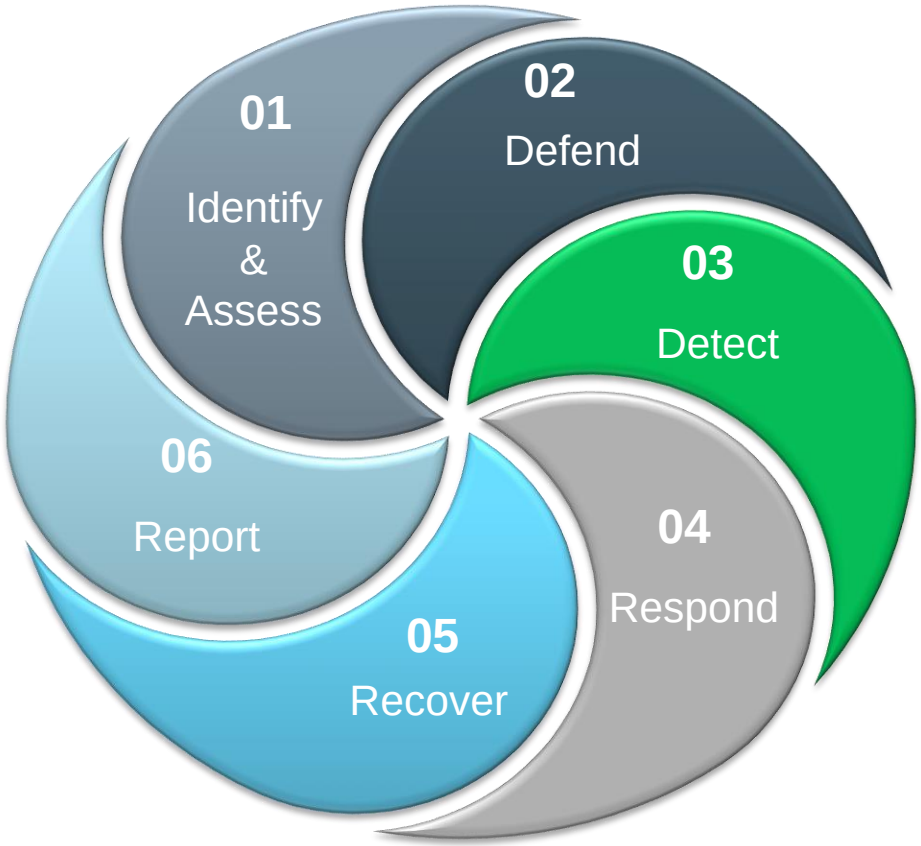
There is **no such thing as perfect security**.

The NIST Cybersecurity Framework Core Functions and the FTC's approach [to data security] **are fully consistent**.

By identifying different risk management practices and defining different levels of implementation, the NIST Framework takes similar approach to the FTC's long-standing Section 5 enforcement.

The NIST Cybersecurity Framework and the FTC, Federal Trade Commission (Aug 2016)

Six Core Functions of Cyber Security Program

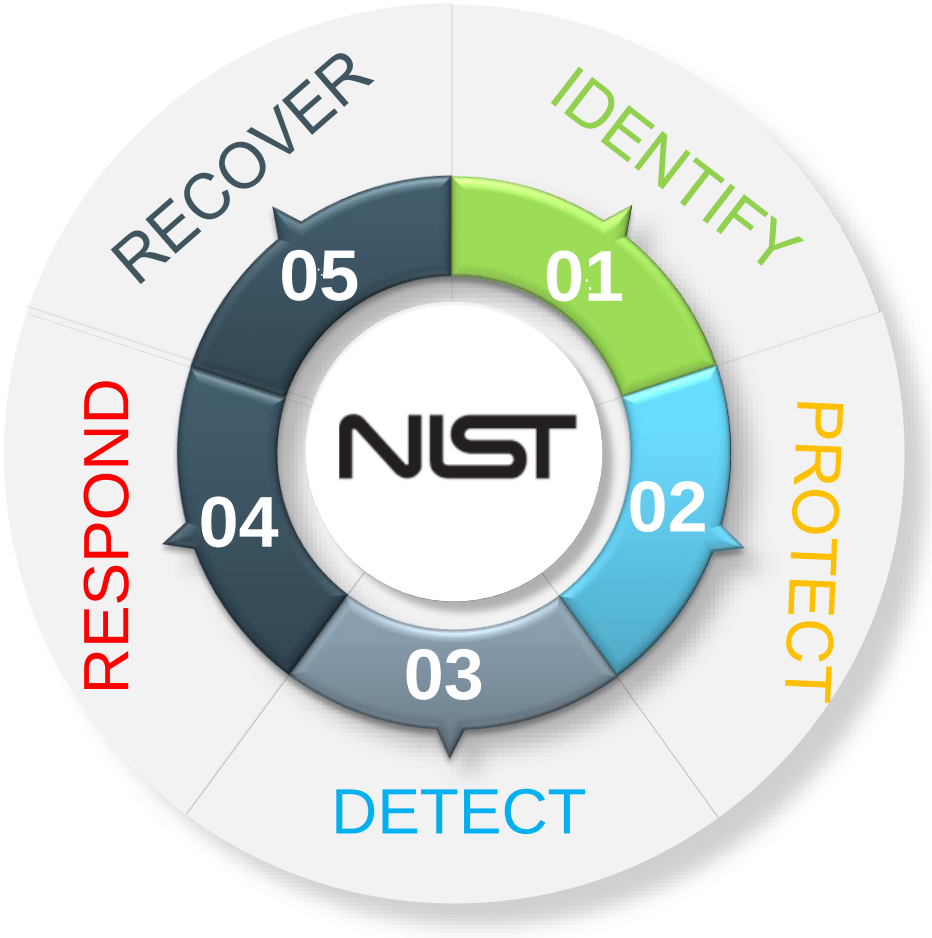


Top 20 Critical Security Controls

1	Asset Inventory
2	Software Inventory
3	Secure Hardware & Software Configurations
4	Continuous Vulnerability Assessment and Remediation
5	Controlled Use of Admin Privileges
6	Maintenance, Monitoring and Analysis of Audit Logs
7	Email and Web Browser Protections
8	Malware Defenses
9	Limitation and Control of Network Ports, Protocols & Services
10	Data Recovery Capability

11	Secure Network Configurations
12	Boundary Defense
13	Data Protection
14	Controlled Access Based on Need to Know
15	Wireless Access Control
16	Account Monitoring and Control
17	Security Skills Assessment and Training
18	Application Software Security
19	Incident Response and Management
20	Penetration Tests and Red Team Exercises

Leverage a Framework



CCPA vs GLBA vs HIPAA

CCPA's Broad Definition of Personal Information

Personal information includes any information that "identifies, relates to, describes, references, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."

1) Name, address, personal identifier, IP address, email address, account name, Social Security number, driver's license number, or passport number
2) Categories of PI described in California's customer records destruction law
3) Characteristics of protected classifications under CA or federal law
4) Commercial information, including records of personal property; products or services purchased, obtained, or considered; or other purchasing or consuming histories or tendencies
5) Biometric information
6) Geolocation data
7) Internet or other electronic network activity, such as browning history, search history, and information regarding a consumer's interaction with a website, application, or advertisement
8) Audio, electronic, visual, thermal, olfactory, or similar information
9) Professional or employment-related information
10) Education information that is subject to the Family Educational Rights and Privacy Act
11) Inferences drawn from any of the information listed above to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes

What Constitutes Personal Information

Key differences in how the CCPA defines “personal information” vs the GLBA and HIPAA

- CCPA’s definition of personal information is distinct from:
  - GLBA’s definition of “nonpublic personal information”
  - HIPAA’s definition of “protected health information”
- CCPA compliance issues beyond the GLBA exception
- CCPA compliance issues beyond the HIPAA exception

How does the Employee Exception Work?

The impact of the CCPA's employee exception

- AB 25 requires that employees, applicants, officers, directors and contractors receive a privacy notice describing the personal information collected and its uses
- Should be delivered by January 1, 2020
- Employee notice will often be separate from applicant notice given differences in information collection and use
- "Director" and "officer" are defined to reference corporations; may not apply to other roles like managers of an LLC or managing partner of a partnership
- "Contractor" is defined as "a natural person who provides any service to a business pursuant to a written contract." [Cal. Civ. C. § 1798.145(c)(2)(A)]

The Security Rule and CCPA- but I am exempt right?

How the HIPAA Security Rule aligns with the CCPA mandates – and how it doesn't

- The **HIPAA Security Rule** is detailed and fairly prescriptive, requiring
  - Specific policies and procedures
  - Risk analysis
  - Appointment of security officer
  - Security provisions to be included in business associate agreements

- CCPA **does not** expressly define "reasonable security" – so far
  - Aside from the AG's 2016 reference to the Critical Security Controls

- HIPAA Security Rule is probably consistent with the CCPA's reasonable security standard
  - As with the FTC's notion of reasonable security under the "unfairness doctrine," the meaning of reasonable security may be defined in future AG enforcement actions rather than express guidance or standards

CCPA and Class Actions

How to strengthen your security incident response plan and security measures to defend against CCPA class action lawsuits

- Consider documenting a determination regarding whether your organization meets the CCPA's "reasonable security" standard
  - Perhaps using the Critical Security Controls as a measure
- Given the likely spike in California security breach class action litigation, this is a good time to review your incident response plan for consistency with best practices
  - How often does your Incident Response Team meet?
  - Do you conduct tabletop exercises?
  - Have your trained your personnel to know a potential security breach when it occurs?

Key Takeaways

“Reasonable” security measures

Real-life examples

1. **Retain Offline Backups of All Critical Systems and Data**
   - Keep at least a 30 day back up offline
   - Physical tapes, external hard drive or controlled segmented network storage

2. **Implement Multi Factor Authentication**
   - Require MFA for all remote access to your office networks
   - Don’t forget cloud based applications such as Email and SaaS services

3. **Properly Configure Your Desktops and Servers Using a Hardening Guide**
   - https://www.cisecurity.org/cis-benchmarks/

4. **Implement Endpoint Monitoring**
   - Deploy a tool to monitor systems for malicious activity *(AV is not enough)*
   - Engage a security vendor to help monitor it *(expertise counts)*

5. **Secure Your Cloud-Based Email**
   - Utilize the Secure Score (O365) or Security Center (Gsuite) to evaluate the security posture of your email.

6. **Establish Appropriate Governance and Communication Channels**
   - Implement information security training and testing
   - Ensure that everyone knows their role in the event of an information security incident

7. **Establish Robust Third-Party Cyber Risk Management Program**
   - Initial due diligence process
   - Review third party service provider access
   - Review contractual obligations
   - Establish period risk assessment processes

Thank you!

For more information about our global locations and services, please visit:
www.kroll.com
www.morganlewis.com

Contacts

Jonathan Fairtlough
Managing Director,
Cyber Risk, Kroll
jfairtlough@kroll.com

Reece Hirsch
Partner, Co-head, Privacy & Cybersecurity Practice,
Morgan Lewis
reece.hirsch@morganlewis.com

Keith Novak
Associate Managing Director,
Cyber Risk, Kroll
keith.novak@kroll.com

Cole Manaster
Senior Associate,
Cyber Risk, Kroll
cole.manaster@kroll.com