The California Consumer Privacy Act, Part 3
Minimum Reasonable Security Practices

June 2019

This SecureTheVillage Webinar brought to you by …

PEPPERDINE | GRAZIADIO BUSINESS SCHOOL

CyRP

CITADEL
INFORMATION GROUP, INC.

Cybersecure SoCal 2019
Cybersecurity is a Team Sport

… a joint presentation of SecureTheVillage and Pepperdine Graziadio Business School

Keynote Speaker: Brad Ross
Fellow at National Institute of Standards and Technology

October 17, 2019 … Mark Your Calendars

The California Consumer Privacy Act Minimum Reasonable Security Practices

- Guide: Stan Stahl, PhD
  - Founder, SecureTheVillage
  - President, Citadel Information Group

- Guest
  - Rachel Capoccia, Partner, Jeffer Mangels Butler & Mitchell LLP

American Cemetery Normandy, France

June 6, 1944 — June 6, 2019

Topics and Outline

- CCPA Overview
  - Likely Changes
- CCPA and the Consequences of “Not Reasonable”
- What Might “Reasonableness” Mean; Reasonableness Candidates
- SecureTheVillage *Minimum Reasonable Security Practices*

STV Resources

Information Security Management ResourceKit

Information Security Management Webinars

SecureTheVillage *Minimum Reasonable Security Practices* (Draft for Review)

CCPA: California Law Codifies Consumer Privacy Rights

- Commencing 1/1/2020, consumers have
  - Right of Disclosure: To request the categories and pieces of information collected, sold, or disclosed about the consumer going back 12 months
  - Right of Deletion: To have certain information deleted, both from the business and any service providers with which the business shared the information.
  - Right to Opt-Out: To opt out of the sale of their information
    - Explicit opt-in under the age of 16 must explicitly opt in to any such sales
  - Right to Be Compensated in Event of Data Breach:
    - Private Right of Action
    - Statutory Damages
    - Definition of PII
- Applies to a for-profit business that collects consumers' personal information that does business in California and that:
  - Has annual gross revenues greater than $25M, or
  - Obtains personal information of 50,000 or more consumers, households or devices annually
  - Derives 50% or more of its annual revenues selling the personal information of consumers
- Includes exceptions for Other Regulatory Privacy, e.g., HIPAA
- Requires new privacy disclosures
- Reasonable security procedures and practices appropriate to the nature of the information being protected qualifies compensation right

Anticipated Changes to the Law

- Clarifies that "personal information" includes information that "is *reasonably* capable of being associated with" a consumer or household
- Broadens the definition of "deidentified" and amends the definition of "personal information" to exclude deidentified or aggregate consumer information
- Requires data brokers to honor consumer opt-outs and any other rights afforded by the CCPA
- Exemptions and Exceptions
  - Personal information from job applicants, employees, contractors, or agents
  - Businesses complying with government requests
  - Sale of information for detection of security incidents or fraud
  - Loyalty or rewards programs
  - Vehicle information retained or shared for purposes of a warranty or recall-related vehicle repair
  - Insurance institutions, agents, and insurance-support organizations from complying with CCPA

The Legal Importance of *Reasonable Security Procedures and Practices*

The California Consumer Privacy Act (CCPA) private right of action establishes statutory damages of between $100 and $750 per incident for consumers whose personal information has been compromised by a breach resulting from the business' "*violation of the duty to implement reasonable security procedures and practices appropriate to the nature of the information to protect the personal information*. (CA Civil Code Section 1798.150(a)(1)).

The statutory exposure for a company with as few as 10,000 "qualifying data elements" is between $1,000,000 and $7,500,000. This combined with the legal duty to acknowledge a breach should one occur, significantly increases the financial risk of such a cyber event.

Begs the Question: What Are "*reasonable security procedures and practices*"

The phrase *implement and maintain reasonable security procedures and practices appears* without definition in both the CCPA and CA Civil Code 1798.81.5.

Consequently, it is not yet known what constitutes reasonable security procedures and practices.

This will emerge as the California legislature amends the Act, as the Attorney General provides guidance, and as case law begins to unfold.

Candidate Descriptors for *Reasonable Security Procedures and Practices*

- NIST Cybersecurity Framework
- Center for Internet Security CIS-20 (c.f., California 2016 Data Breach Report)
- New York State Department of Financial Services, 23 NYCRR 500
- NIST 800-171
- Payment Card Industry's Data Security Standard (PCI DSS)
- HIPAA & Gramm-Leach-Bliley
- ISO 27001, 02 Certification

- While each may be *reasonable* for some organizations, none are *reasonable* for all organizations
  - Too Strong
  - Too Weak
  - Inadequately defined

Starting Point: The Essence of Reasonableness

The number one thing at the Board level and CEO level is to take cybersecurity as seriously as you take business operations and financial operations. It's not good enough to go to your CIO and say "are we good to go." You've got to be able to ask questions and understand the answers.

Major Gen Brett Williams, U.S. Air Force (Ret)
This Week with George Stephanopoulos, December 2014

SecureTheVillage's *Minimum Reasonable Security Practices*

- A *minimum set of security practices* that a company (subject to CCPA) must implement and maintain for it to claim that it has reasonable security procedures and practices.
  - Based upon above standards
  - Analogous to our earlier *Basic IT Security Management Practices*
  - Straw man in community dialogue
    - Plan to send to Atty General Becerra
  - Baseline for companies
  - Guide for attorneys
  - Guide for insurance providers
  - Guide to financial institutions

https://mrsp.securethevillage.org/

Categories: Minimum Reasonable Information Security Practices

- Risk-Based Information Security Management
  - Information Security Subject Matter Expertise
  - Security Management of Sensitive and Private Information
  - SecureTheHuman
  - Security Management of the IT Interface
  - Security Management of the IT Infrastructure
  - Third-Party Security Assurance
  - Information Resilience
  - Information Security Governance

What We Need: Take a Look. Send Us Feedback.

- Review
- Comment
- Provide Feedback

https://mrsp.securethevillage.org/

Next Webinar: July 25

Risk Management

- NIST Risk Management Framework
- Pepperdine Graziadio Business School CyRP Program
- Cybersecure SoCal 2019

Guests:

- Howard Miller, LBW Insurance, SecureTheVillage Board, CyRP Advisory Board

- Charla Griffy-Brown, Professor, Information Systems and Technology Management, Chair CyRP Advisory Board

No Webinar in August

SecureTheVillage Webinar Series

- Information Security Management Guidance
  - Practical
  - Real-World
  - How-To
  - Actionable
- SecureTheVillage ResourceKit
- First Thursday of month, 10AM Pacific

SecureTheVillage: Turning People and Organizations into Cyber Guardians

Monthly Webinar Series: Provides Practical Real-World Actionable How-To Information Security Management Guidance.

Executive Focus Groups: Designed to assist Chief Executives understand how to turn their organization into Cyber Guardians and create a cyber resilient culture.

Information Security Management and Leadership ResourceKit: A practical guide for implementing an information security management and leadership program in your organization.

Code of Basic IT Security Management Practices: A set of basic IT security management practices that are so basic that a failure to implement them puts the organization at a dangerous and unnecessary risk of a costly information incident.

Minimum Reasonable Security Practices: A set of information security management practices so basic as to be necessary for a claim that one's information security practices and procedures are reasonable. *Developed in support of CCPA.*

Community-Based Programs: Train the broader community in basic cybersecurity defense practices for themselves and their families, helping them become cyber-aware citizens.

Visit us at: *SecureTheVillage.org*

For More Information …

Stan Stahl, SecureTheVillage & Citadel Information Group
Stan@SecureTheVillage.org
323-428-0441

Rachel Capoccia, Partner, Jeffer Mangels Butler & Mitchell
RCapoccia@jmbm.com
310.201.3521

FREE Citadel *Cybersecurity News of the Week & Weekend Vulnerability and Patch Report*
https://Citadel-Information.com

Follow SecureTheVillage on LinkedIn: https://www.linkedin.com/company/secure-the-village
Follow Citadel on LinkedIn: https://www.linkedin.com/company/citadel-information-group

For Marketing / Sponsorship Opportunities
Email us at info@securethevillage.org. Put *Sponsor Opportunity* in Subject
Visit us at https://securethevillage.org/sponsorship-opportunities/

Thank You

The California Consumer Privacy Act, Part 3
Minimum Reasonable Security Practices

June 2019