CYBER SECURITY LAWS

How to Keep Up With Ever-Changing Technology Laws

By: Joshua Bordin-Wosk (Bordin Martorell LLP) and Richard McAbee (Carl Warren)

PARMA Conference – February 13, 2017

Overview

1. Privacy Concerns Relating to Cyber Security
2. Employees' Right to Privacy from Employer
3. Protection from Outside Attacks
   a. Common Causes
   b. What You Can Do
   c. What Your Employer Can Do
   d. What Laws Protect You
4. What To Do In Case of Breach

1. Privacy Concerns Relating to Cyber Security

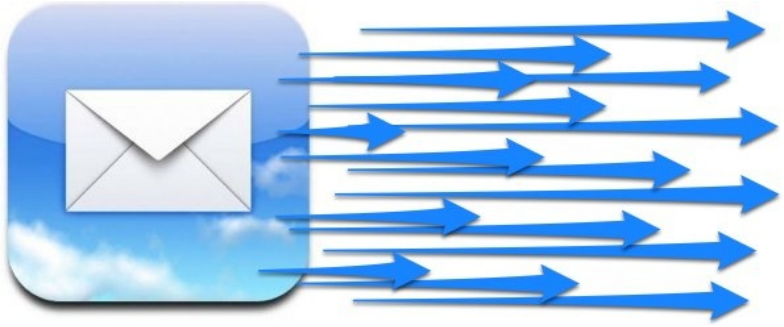
- Several laws are in place that protect privacy rights:
  - California Penal Code section 502
    - Provides criminal charges and civil relief for misuse of computers which result violations of privacy
  - California Government Code section 11015.5
    - Establishes guidelines for governmental agencies collecting personal information electronically
  - California Government Code section 11019.9
    - Requires government agencies to implement permanent privacy policies to ensure personal information is protected

2. Employees' Right to Privacy from Employer – Common Questions

1. Can employers monitor emails?

2. Can employers monitor phone calls?

3. Can employers look through cell phones?



Employees' Right to Privacy – Emails

- No right to privacy where:
  1. The electronic means used belongs to the employer;
  2. Employer advised employees that communications using electronic means are not private, may be monitored, and may be used for business purposes only; and
  3. Employee is aware of and agrees to these conditions.

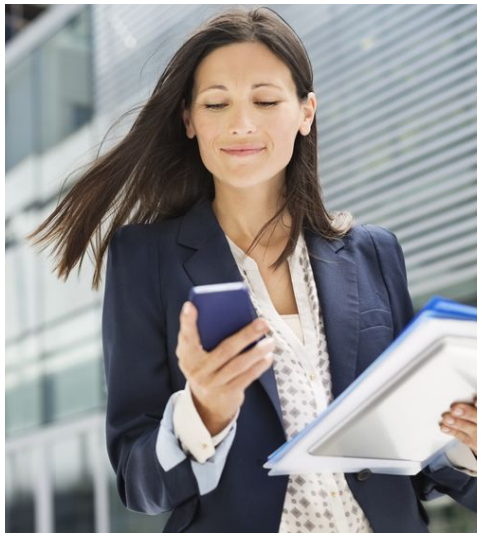
(*Holmes v. Petrovich Development Co., LLC* (2011) 191 Cal.App.4th 1047, 1068.)

Employees' Right to Privacy – Phone Calls

- California's wiretapping law is a "two-party consent" law

- Recording or eavesdropping on a confidential communication, including a private conversation or telephone call, without the consent of all parties to the conversation is a crime (Cal. Penal Code, § 632.)

Employees' Right to Privacy – Cell Phones



- Law has not specifically addressed whether an employer can search an employee's company-issued cell phone
- However, no right to privacy where an employee signed an electronics policy agreeing that employer could monitor computer usage, and then used an employer-issued laptop to work from home.

  (*TBG Ins. Services Corp. v. Super. Ct.* (2002) 96 Cal.App.4th 443, 445.)
- Same argument can be made for company-issued cell-phones

Expanded Protection for Government Employees?

- Unlike private-sector employees, government employees' right to be free from unreasonable searches and seizures applies.

- The Fourth Amendment protects from intrusion by the Government, even when the Government acts in its capacity as an employer (*Ontario v. Quon* (2010) 560 U.S. 746.)

- Where a government employee claims their privacy rights were violated, courts will look at (1) how the search was performed; (2) why the search happened; and (3) whether the employee assumed their use of the electronics was private.

3. Protection from Outside Attacks

- To prevent outsiders from breaching into and gaining access to personal information, be aware of:

  a. Common Causes

  b. What Employees Can Do

  c. What Employers Can Do

  d. What Laws Protect You

a. Common Causes of Data Breaches

i. Human Error

ii. Lack of Security

Common Causes –
i. Human Error

- Human error has resulted in monumental breaches:
  - Theft or loss of physical property
    - Veteran's Administration (2006) – 26.5 million discharged veterans' records, including name, SSN & date of birth, stolen from the home of an employee who improperly took the material home
  - Suspicious emails
    - Sony Picture (2014) – "Phishing" emails used to hack Sony Pictures, leading to the cancellation/delay of the film "The Interview"

Common Causes –
ii. Lack of Security

- Lack of security has also led to massive breaches:
  - <u>Insufficient virus protection and/or firewalls which lead to hacking</u>
    - Ashley Madison (2015) – Infidelity website hacked, breaching personal information of 37 million users; hackers threatened to release user' names and information if website did not shut down
    - Target (2013) – Software installed on credit/debit card machines led to breach of payment and contact information for 110 million people, costing $162 million

b. What Employees Can Do –
Preventing Breaches by Avoiding Human Error

- Don’t take home work property without permission
- If you do take home work property, keep careful track of it
- If work property is compromised, report it immediately
- Know your work’s protocol regarding how to identify and handle suspicious emails

Avoiding Human Error –
Suspicious Emails

- Phishing emails typically contain one of several key giveaways.

- Be aware of:
  1. Grammar Errors and Misspellings
  2. Warnings that you must “ACT NOW”
  3. Offers from personal email accounts (i.e. yahoo.com, gmail.com, etc.)
  4. Strange links
  5. Unusual instructions (i.e. “change your password via this link”, rather than “contact customer service”)
  6. Discrepancies between the fine print and the content of the email

c. What Employers Can Do –
Ways to Fight Cyber Crime

i. Protect the perimeter
ii. Train employees
iii. Build a firewall
iv. Update software regularly
v. Change passwords often
vi. Secure your networks
vii. Monitor social networks
viii. Encrypt data
ix. Confirm your vendor's security
x. Buy the right insurance

i. Protect The Perimeter

- Guard your physical perimeter to prevent hackers from accessing sensitive data and your entity's computer network
- Consider whether your Wi-Fi signal and computer network are accessible from outside your facility and what protections you need to keep out unauthorized users
- Look at how easy it is to get inside secure areas of your location and whether access cards are stored securely

ii. Train Employees

- Educate your team because employees are your organization's first line of defense against cybercriminals
- Provide training in the workplace for all levels of employees
- Remember that almost everyone carries a smartphone or tablet these days, and most phones don't have the same security software that computers do

iii. Build A Firewall

- Activate your firewall to block connections that are used to hack into your system and deliver viruses

- You may need to evaluate what kind of firewall to use at different points on your system and whether you also need better host security

iv. Update Software Regularly

- Install and regularly update spyware, anti-virus and malware software to help prevent and detect any of those from affecting your computers

- Ensure that all government-owned devices also have the most up-to-date security software. If your entity allows employees to access government information on their personal electronic devices, have a policy that requires security software with regular updates on those devices as well

v. Change Passwords Often

- Use stronger passwords of 8-10 characters that include letters, numbers and special characters
- Change those passwords regularly on your network, and require all employees to change their passwords regularly as well
- If you have a guest wireless network, you should change that password often, for example, weekly, and only allow the connection to remain open for a limited amount of time.

vi. Secure your networks

- Secure your Wi-Fi networks to prevent hackers from accessing your servers or using your internet connection without your knowledge
- An even more basic protection is to consider whether you need a wireless network at all
- One government office has no wireless network accessibility in its building for visitors or employees
- Only a limited number of employees have access to email on electronic devices, and those who are authorized to work at home must use a VPN on a wired network

vii. Monitor Social Networks

- Set social network profiles to private and check security settings
- Be mindful of what information you post online
- If you have a social media site, for example a Facebook page, control who can post on that page, and whether an administrator has to review and authorize posts

viii. Encrypt Data

- Encrypt your most sensitive data, make a backup and store it in a fireproof safe or off-site.
- Use a dedicated computer for all sensitive information.
- Be sure you understand what data you control that is sensitive.

ix. Confirm Your Vendor's Security

- Carefully select online computing services, because any information you share with them can be compromised by their system
- Require system security and regular updates as part of your contract with any vendor for computer services as well as any suppliers that might have access to your system
- If you allow vendors to upload information to your computer network, require their systems to be secure as well

x. Buy The Right Insurance

- Acquire cyber insurance to cover losses in case of a breach or fraud
- Broker should review the client's insurance package and ensure that the appropriate coverage is in place
- Remember that one cyber incident can shut down your entity
- Consider what kind of protection your entity needs if a supplier or vendor has a cyber incident

d. What Laws Protect You –
Ensuring Data Storage Has Sufficient Security

- California initially enacted laws that focused on reporting breaches to consumers (Cal. Civil Code sections 1798.29 & 1798.82)
- To increase protection, California bolstered laws intended to prevent breaches before they occurred (Cal. Civil Code section 1798.81.5)
- Going into the future, California looks to increase minimum security standards, strengthen existing protections, and collaborate with other states to provide uniform standards for businesses and agencies

Laws Initially Focus on Reporting Post-Breach

Model Security Breach Notification Form

[NAME OF INSTITUTION / LOGO] Date: [insert date]	
NOTICE OF DATA BREACH	
What Happened?	
What Information Was Involved?	
What We Are Doing.	
What You Can Do.	
Other Important Information. [insert other important information]	
For More Information.	Call [telephone number] or go to [Internet Web Site]

- California Civil Code sections 1798.29 & 1798.82 require reporting of any breach of the security system by unauthorized person(s) who obtain personal information
- **Section 1798.29** applies to governmental agencies that own, license or maintain computerized data containing personal information
- **Section 1798.82** applies to any person or business who owns or licenses computerized data containing personal information

California Civil Code sections 1798.29 & 1798.82 – Intent

- Lawmakers thought that the effort, expense and shame in having to report security breaches would influence persons, businesses, and agencies who house computerized personal information to protect that information

- However, this approach was largely unsuccessful…

Widespread Data Breaches

Between 2012 and 2015:

- 657 Total Data Breaches, affecting 49 million Californians
- 3/5 Californians were victims of data breach in 2015
- Government entities accounted for 5% of breaches between 2012-2015

Increase in Breaches:

- 2012 = 131 Breaches involving 2.6 million records → 2015 = 178 Breaches involving 24 million records

Cyber Security Readiness Study (Hiscox) Finds Widespread Shortcomings

a. Incidence of attacks is high
b. Costs range to over $500,000 per incident
c. Cyber security spending is rising fast

a. Incidence Of Attacks Is High

- More than half (57%) of organizations have experienced a cyber-attack in the past year
- Two in five (42%) have had to deal with two or more breaches
- Larger companies are targeted most often
- Nearly half (46%) of businesses took two days or more to get back to business as usual

b. Costs Range To Over $500,000 Per Incident

- The average cost of cyber security incidents experienced in the past 12 months ranges between $22,000 to $500,000 for the largest organizations
- These figures only consider the direct costs of an incident
- The impact on business reputation and customer confidence can be much greater

c. Cyber Security Spending Is Rising Fast

- The majority of cyber security budgets (59%) are set to increase by 5% or more over the coming 12 months
- One in five firms (21%) will lift spending by a double-digit amount
- Attacks prompt more spending on technology
- Around a quarter of firms that experienced a cyber-attack responded by increasing their spending on prevention or detection technologies (24% and 23% respectively)

Focus of Laws Shift to Preventing Breaches

- California Civil Code section 1798.81.5 was amended in 2015 to add businesses that *maintain* personal information, as well as businesses that own and license personal information

- Purpose of the section is "to ensure that personal information about California residents is protected"

- To achieve its goal, the section is meant to "encourage businesses that own, license, or maintain personal information about Californians to provide ***reasonable security*** for that information."

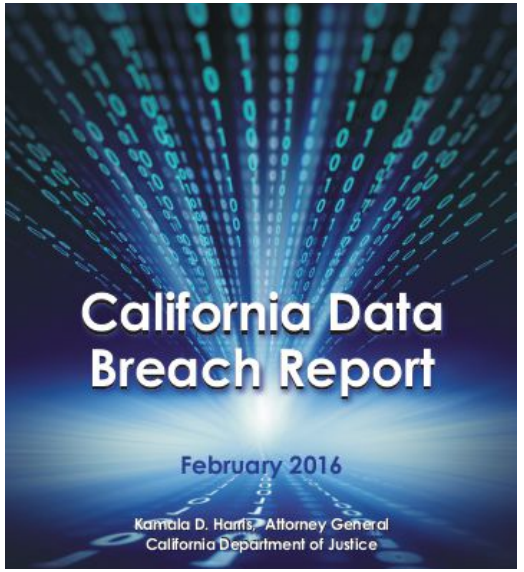
California Civil Code section 1798.81.5

- Requires businesses that store personal information to have **reasonable security procedures** to protect that information

- Key = <u>Reasonable Security Procedures</u>

Reasonable Security Procedures – What Does This Mean?

- No set definition, but…
- The California Attorney General published the California Data Breach Report, which stated:
  - 20 "controls" from the Center for Internet Security's ("CIS") Critical Security Controls define a **minimum level of information security** that all organizations that collect or maintain personal information should meet.
  - *Failure* to implement all Controls that apply to an organization's environment constitutes a **lack of reasonable security** – a.k.a. violation of Civil Code section 1798.81.5



CIS's Critical Security Controls

- The report noted that the Controls are listed in priority order, and act in concert (i.e. to protect data on laptops and other portable devices (CSC 12), an organization must first know what devices it has and where they are (CSC 1).)
- CIS states that by implementing the top 5 controls, companies/ agencies can reduce their risk of cyberattack by around 85%, and that by implementing all 20 CIS Controls, companies increase the risk reduction to around 94%.

CSC 1	Inventory of Authorized and Unauthorized Devices
CSC 2	Inventory of Authorized and Unauthorized Software
CSC 3	Secure configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
CSC 4	Continuous Vulnerability Assessment and Remediation
CSC 5	Controlled Use of Administrative Privileges
CSC 6	Maintenance, Monitoring, and Analysis of Audit Logs
CSC 7	Email and Web Browser Protection
CSC 8	Malware Defenses
CSC 9	Limitation and Control of Network Ports, Protocols, and Services
CSC 10	Data Recovery Capability
CSC 11	Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
CSC 12	Boundary Defense
CSC 13	Data Protection
CSC 14	Controlled Access Based on the Need to Know
CSC 15	Wireless Access Control
CSC 16	Account monitoring and Control
CSC 17	Security Skills Assessment and Appropriate Training to Fill Gaps
CSC 18	Application Software Security
CSC 19	Incident Response and Management
CSC 20	Penetration Tests and Red Team Exercises

Cyber Security Laws Passed by the Legislature

- **California Assembly Bill No. 2623** – "State Agencies" and "State Entities" (per Gov. Code 11546.1) must submit a summary of its actual and projected information security costs
- **California Senate Bill No. 1444** – Requires state agencies to inventory personal information that is either stored or transmitted by the agency. Calls for agencies to establish procedures to facilitate communication between an incident response team, agency officials, and individuals affected by a breach
- **California Senate Bill No. 1137** – Updates the Criminal Code to criminalize individuals who knowingly put ransomware on a computer's system, network or data

4. What To Do In Case of Breach

Implement a Cyber-Breach communication plan. This should include:

a. Improved technology security

b. Financial protection and mitigation

c. Rebuilding trust through effective communications

a. Improved Technology Security

- Today's technology has increasing dependence on the use of mobile devices and storage solutions such as cloud-based software, with security measures based on keys and certificates.

- Through these keys and certificates, hackers gain access.

b. Financial protection

- Although there are a variety of technical solutions you can employ to protect against a cyber threat, there are still other risk strategies that should be considered should a breach occur
- Each policy differs in scope and coverage; however, generally first-party liabilities cover costs associated with the actual breach (forensic investigation, profit/loss and legal advice)
- Third-party liabilities commonly cover damages caused by the breach (legal defense, public relations initiatives and regulatory response)

c. Rebuilding Trust

- With improved security measures and mitigated financial impact comes the need for reputation management and the ability to rebuild trust damaged through a breach

- Preparing communication plans and messaging in advance, whether through internal means or in partnership with a firm will position organizations to effectively weather the storm while minimizing overall damage to the Government Entity

c. Rebuilding Trust –
Crisis Communication

- To begin your crisis communications planning, begin with these four tips:
  i. Bring the Team Together
  ii. Brainstorm
  iii. Assign Tasks

i. Bring the Team Together

- Begin your communications plan through the identification of a crisis team.
- Identify who should be at the table when a breach occurs.
- The crisis team should include executive representation, legal, information technology, human resources, finance, operations and communications.
- Bringing these decision-makers together before, during and after the crisis will create a cohesive approach to the crisis along with consistent messaging for both internal and external stakeholders.
- Include your risk manager and insurance agent or broker.

i. Bring the Team Together –
Post-Event Evaluation

- Conduct a post-evaluation crisis to review corrective actions and formal and informal communications throughout the incident.
- To mitigate damage, specifically from a cyber breach, prepare for a crisis immediately. Begin with an evaluation of the technology security plan and protocols. Implementing stricter security software keys and certifications is the best course of action.
- Understanding that a breach is likely to happen, safeguarding against financial loss is also a positive step more and more government entities are implementing. A proactive approach to designing communication strategies will reduce lost trust and protect your entity's reputation.

ii. Brainstorm

- Every quality crisis communications plan is organized, comprehensive and specific to your organization.
- While planning, think through and identify the specific crisis your organization could face.
- For healthcare, consider the various HIPPA scenarios that you could experience.
- For legal, how could government claims/records be compromised?
- As the team works through their potential concerns, they establish the protocols necessary to mitigate the process.

iii. Assign Tasks

- Every staff member has a role to play in an emergency, whether it's an active role in the ongoing crisis or in supporting the post-crisis efforts.
- Determine the tasks that you'll be required to do regardless of the challenges you face.
- Business operations (payroll, for instance) must continue with as little disruption as possible.
- Employees play a significant role in your communications, whether you want them to or not.
- Keeping them engaged and informed is a positive step toward a consistent message.
- Be sure to clearly identify who will do what prior to a crisis and ensure that employees know their roles and how to execute these responsibilities well in advance of an emergency.

Review

- Cyber Security laws that affect privacy rights include California Penal Code section 502, and California Government Code sections 11015.5 & 11019.9
- To protect your privacy, know what your employer can and cannot do with your digital personal information
- To be protected from outside cyber attacks, be aware of common issues, prevent human error, and be familiar with what your employer is doing to comply with laws to prevent breaches
- Know what to do in case of a breach, and how to minimize the damage