IMPLEMENTING THREAT-BASED CYBERSECURITY TO MITIGATE DATA BREACHES & DAMAGES FROM CCPA LAW SUITS

BDO

CCPA BACKGROUND

The new California Consumer Privacy Act (CCPA) goes into effect on January 1, 2020. Businesses subject to the new California privacy law need to ensure compliance with numerous new cybersecurity requirements. These additional regulatory burdens on businesses operating in California present a potential gold mine for plaintiff's firms. These firms could leverage CCPA's private right action, which imposes significant statutory damages, to pursue a potential tidal wave of class action cases. Any business subject to the CCPA, may be held liable if California consumers can demonstrate that their personal identifiable information (PII), with an extremely broad definition of PII, was affected by a cyber data breach, and resulted from the business's neglect or failure to implement "reasonable security."

THE WORLD WE LIVE IN

According to a recent report issued by the U.S. Security Exchange Commission (SEC), the average cost of a cyber data breach is $7.5 million and continues to increase in value year over year. While all organizations are potential targets of cyber-attacks, the industries which possess the most valuable data are the biggest targets including: financial services, healthcare, government, automotive, manufacturing and retail. All organizations possess PII, valuable information assets, which may include: intellectual property, financial payment information, client information, supply chain information, protected health information (PHI), and/or payment card information (PCI), just to name a few.

IMPLEMENTING THREAT-BASED CYBERSECURITY

Businesses operating in California and subject to the CCPA will need to implement a proactive threat-based cybersecurity program, which begins by understanding the cyber threats (including threat actors, vectors, tactics, techniques, and procedures). Then it creates a customized cyber defense plan, which effectively aligns the business's threat profile, budget and schedule. In implementing a threat-based cybersecurity program, a business can limit the risk of CCPA class action litigation, by demonstrating that they have taken the necessary and appropriate information security actions to provide "reasonable security" to protect California consumers' personal information.

To successfully implement a threat-based cybersecurity program, a business must take specific cybersecurity actions before, during and after a data breach, including the following:

BEFORE THE DATA BREACH

Select one or two independent firms with extensive cybersecurity advanced diagnostic capabilities, cyber threat intelligence data collection and analysis capabilities, cybersecurity advisory expertise, and/or managed security services to do the following proactive actions:

- Conduct a **dark web analysis** of the business's key personnel, and selected supply chain partners to gather potential threat intelligence information
- Conduct a **social media analysis** of the business's key personnel to gather threat intelligence information
- Perform a **vulnerability assessment** of the business's computers and remote devices
- Conduct **penetration testing** on the business's network, software applications and endpoints
- Perform an email **spear-phishing campaign** to test the business's employees' level of cyber awareness
- Conduct a **security software tools assessment** to ensure expensive security software is properly configured, operating effectively and employees are adequately trained
- Conduct a **cyber maturity assessment** or (risk assessment) to evaluate the business's information security and privacy program's policies, plans, and procedures vs. industry standards or cybersecurity risk management frameworks
- Provide **cybersecurity education and training** to all employees
- Perform a **cyber liability insurance coverage adequacy assessment**
- Develop and test an **cyber incident response plan**
- Develop and test a **business continuity plan** (BCP)
- Implement **data encryption and multi-factor authentication** (MFA)
- Implement a timely **software patch management program**

Before a data breach occurs, it is vital to take cybersecurity actions to ensure "reasonable security" exists. All cybersecurity assessments and related findings should be performed and delivered under attorney-client privilege. The cyber diagnostic assessments, listed under Before the Data Breach, should all be focused on identifying potential cyber vulnerabilities within the business, which could lead to cyber data breaches. The primary purpose of the cybersecurity diagnostic assessments are to gain a clear understanding of the current threat profile the business is facing, identify the organization's information security vulnerabilities to cyber-attacks and to develop a customized cyber defense plan of action.

DURING THE DATA BREACH

Recognizing that each data breach is somewhat unique, there are certain key actions that need to be taken as soon as possible after the initial determination that a cyber intrusion has occurred and that there was a compromise and/or exfiltration of data, the malicious encryption of data, or destruction of data has occurred, including the following actions:

- Implement your business's cyber incident response plan and notify your attorney
- Identify the points of infiltration, exfiltration and extent of contaminated hardware and software
- Contain the spread of the malware or virus
- Eradicate the malware, ransomware or virus
- Recover the data as quickly as possible
- Notify local law enforcement and FBI as appropriate
- Restore information system to full operational capacity via back-up system
- Conduct an email system cyber-attack assessment - to check for advanced persistent threat malware
- Conduct computer/mobile device vulnerability scanning - to check for viruses and malware
- Hire an independent firm to conduct a cyber incident investigation
- Document the actual incident response actions and lessons learned
- Prepare and submit a cyber liability insurance claim
- Conduct on-going monitoring, detection, and incident response 24 x 7 x 365 either internally or via a managed security services provider (MSSP)

AFTER THE DATA BREACH

Take the following cybersecurity remediation actions as necessary and appropriate:

- Conduct a full risk assessment
- Provide cybersecurity education and training program for all employees
- Perform or hire a qualified managed security services provider (MSSP) to:
  - Provide managed monitoring detection & incident response services – 24x7x365
  - Provide threat intelligence services
  - Assess third-party vendor cyber risks
  - Provide full data encryption
  - Use multi-factor authentication (MFA)
  - Implement an incident response plan (IRP)
  - Establish a business continuity plan (BCP) with full off-line back-up system
  - Develop and test a disaster recovery plan (DRP)

SUMMARY

The risk of a data breach negatively impacting a company's reputation and market value is both real and ever increasing. With the additional enactment of the CCPA we could see a significant increase in class action litigations in California, focused on data breaches and the CCPA imposed legal damages. Thus, all businesses subject to the CCPA need to implement a threat-based cybersecurity program to fully identify and understand the value of the information assets they possess, recognize the cyber threats they are facing, calculate the related risk factors and then implement a customized defense plan. By implementing a threat-based program, businesses can clearly demonstrate that they have provided "reasonable security" for the protection of consumers' personal information, while ensuring shareholders that they are protecting vital information assets required to both survive and thrive in a digital marketplace.

CONTACT

GREGORY GARRETT
Head of U.S. and International Cybersecurity Advisory Services
703-770-1019
ggarrett@bdo.com

GREG SCHU
Partner, Governance, Risk & Compliance
612-367-3045
gschu@bdo.com

MIKE STIGLIANESE
Managing Director, Head of Cyber Risk Assessments
212-817-1782
mstiglianese@bdo.com

ERIC CHUANG
Managing Director, Head of Cyber Incident Response
703-245-8687
echuang@bdo.com