THOMSON REUTERS

Westlaw®

Cybersecurity, privacy and everything in between: How 2018 has changed the landscape

By Jeffrey M. Dennis, Esq., and Amtoj S. Randhawa, Esq., *Newmeyer & Dillion*

DECEMBER 2018

2018 has been a pivotal year for consumer data protection and cybersecurity, with sweeping new laws being passed to ensure increased consumer data and privacy around the world. If you, like most people, have not tracked each and every development, there is no need to panic.

Below are our top five consumer data protection, privacy and cybersecurity issues for 2018 that you should be aware of, as well as practical steps that can be taken to ensure your company is in compliance with new laws and regulations, and is keeping up with the latest trends.

1. ACTIVATION OF THE GDPR

The General Data Protection Regulation is a strict, comprehensive framework of security regulations enacted by the European Union to protect its citizens. It went into effect May 25. The GDPR provides a blueprint for a combination of required legal, technological and work habits within an organization.

> U.S. companies must analyze their data and processes to determine whether compliance with the GDPR is necessary.

While the GDPR was enacted by the EU to protect its own citizens, it applies to any organization, including those situated in the U.S., that collects or processes data of EU citizens. Therefore, U.S. companies must analyze their data and processes to determine whether compliance with the GDPR is necessary.

The GDPR applies directly to the processing of personal data in the context of activities of an establishment of a controller or processor in the EU, regardless of whether the processing takes place in the EU.

Additionally, specific GDPR provisions apply to non-EU companies if their processing activities relate to the offering of goods or services (irrespective of whether a payment of the data subject is required) or to the monitoring the behavior of individuals within the EU. If a company falls within one or both categories, compliance with the GDPR is required.

If a company fails to comply with the GDPR, the supervisory authority in the impacted EU nation has the power to impose severe administrative fines. The extent of the violation and type of personal data involved will dictate the severity of the fine imposed.

For example, under the GDPR, a company could be subject to administrative fines up to 20 million euros (about $22.75 million) or up to 4 percent of the company's total worldwide annual revenue in the preceding financial year. These fines would be crippling to most companies.

If a company determines it falls within the purview of the GDPR, there are simple steps it can take to begin ensuring it is in compliance.

At a minimum, a company should begin by:

- Reviewing and analyzing data repositories for sensitive data;
- Performing an analysis/accounting of procedure for data collection; and
- Creating an oversight committee dedicated to data activities and compliance.

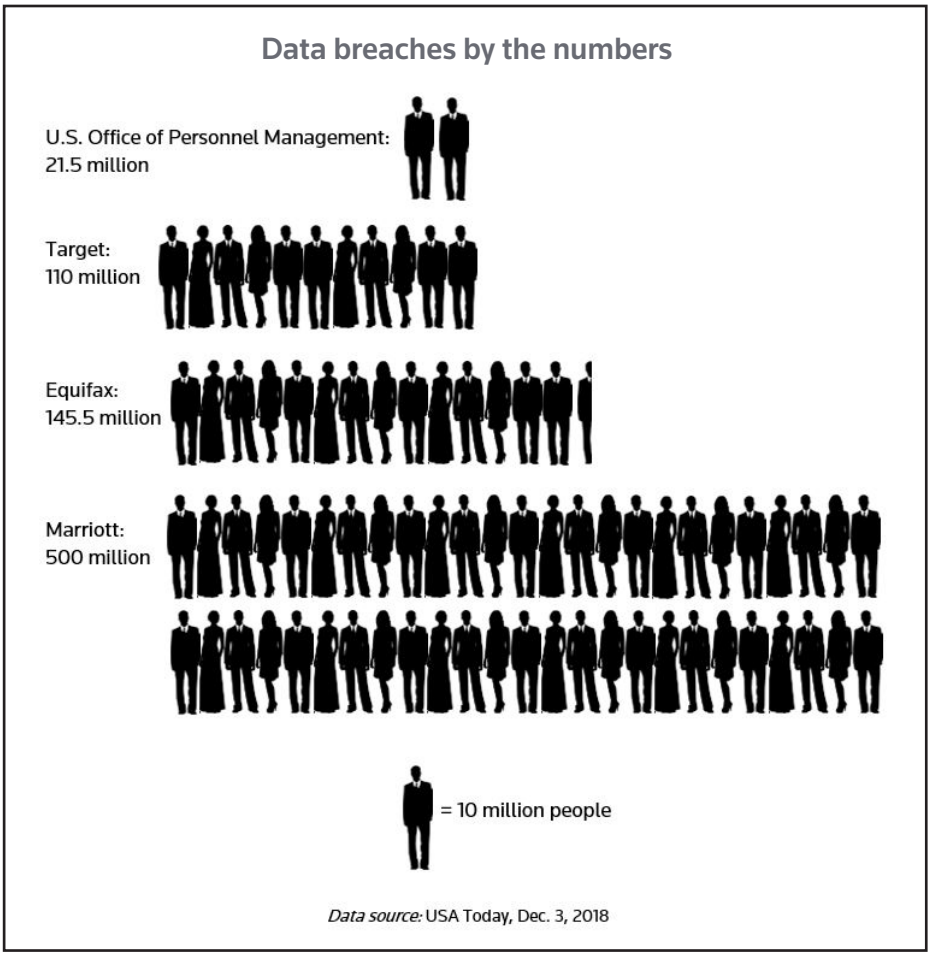
2. CALIFORNIA FOLLOWS THE EU'S LEAD

It is no secret that California has been at the forefront of consumer data protection and cybersecurity reform. In June, the California Legislature passed the California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.175.

When the CCPA becomes effective Jan. 1, 2020, it will force significant changes on companies that collect and sell personal data and will provide consumers with greater protection and control over their personal data.

The new California law provides consumers with certain basic rights when it comes to their personal information. These include:

- The right to ask a business to disclose the categories and specific pieces of personal information the business has collected.
- The right to have a business delete any personal information it has collected.



- The right to know what personal information a business has collected about them, where the data was sourced, what it is being used for, whether it is being sold or disclosed and to whom it is being sold or disclosed.
- The right to opt out of allowing a business to sell or disclose their personal information to third parties for a business purpose.
- The right to receive equal service and pricing from a business, even if exercising privacy rights under the law.

The CCPA will apply to for-profit businesses that collect and control California residents' personal information, do business in the state and meet any of the following criteria:

- Have annual gross revenues in excess of $25 million.
- Receive or disclose personal information of 50,000 or more California residents, households or devices annually.
- Derive 50 percent or more of their annual revenue from selling California residents' personal information.

The law was intentionally drafted to encompass not only large companies with an online presence and larger brick-and-mortar stores, but also smaller companies, even if they are not physically present in California.

By January 2020, all businesses that meet at least one of the three conditions above will need to have methods in place to monitor their data collecting, and have data-sharing practices and resources in place to provide requested information to consumers quickly.

If your company does any business in California, or deals with the data of California citizens, you must pay immediate attention to the requirements of the CCPA.

Among other things, companies subject to the CCPA will need to:

- Determine what personal data they are collecting from individuals and for what purpose, where the data comes from, whether it is being sold or disclosed, and to whom.

- Provide at least two methods for consumers to submit requests for disclosure, including, at a minimum, a toll-free telephone number and website address.
- Disclose requested information free of charge to the consumer within 45 days after receiving the request, subject to extension.
- Disclose if they sell consumer data to third parties and give consumers the ability to opt out of the sale by placing a link titled "Do Not Sell My Personal Information" on their website's home page.
- Update their privacy policies prior to Jan. 1, 2020, and every 12 months thereafter to make the disclosures the law requires.
- Refrain from selling personal information of a consumer younger than 16 without the consumer's affirmative consent (or, if younger than 13, the consent of their parents).

In addition, the CCPA requires companies to take more precautions to protect the personal data they collect in an effort to prevent the exposure of personal information to data breaches.

Specifically, the CCPA requires that companies "implement and maintain reasonable security procedures and practices" to ensure that consumers' private information is not exposed in a security breach.

If your company does any business in California or deals with the data of California citizens, you must pay immediate attention to the requirements of the CCPA.

Likewise, all U.S. companies should familiarize themselves with the CCPA. In all likelihood, numerous states will follow California's lead and enact similar legislation. Much like data breach notification requirements, California has set a standard that other states will follow.

3. CONTINUED FALLOUT FROM THE EQUIFAX DATA BREACH

The Equifax data breach of 2017 affected over 145 million U.S. customers and is widely regarded as one of the largest cybersecurity breaches in U.S. history.

Equifax's failure to properly update and patch its computer systems, failure to mitigate damages and cut access when suspicious web activity was detected, and failure to discover follow-up scan vulnerabilities all resulted in the catastrophic breach that made national news headlines. Equifax not only failed to take appropriate precautionary measures to protect its clients' data, but also failed to appropriately respond to the breach.

The Equifax debacle has taught us that companies must focus on three key areas with respect to data security: prevention, maintenance and response. Prevention includes the implementation of comprehensive internal policies, penetration testing, and device update and management protocols.

Maintenance includes routinely evaluating a company's cybersecurity measures to ensure they are up to date and can combat continuously evolving threats.

Finally, a company must think of cyberbreaches in the context of "when" rather than "if." A thorough and comprehensive response plan must be implemented so that a company can appropriately respond after a breach.

4. INCREASED OBLIGATIONS FOR PROFESSIONAL SERVICE PROVIDERS

In 2018, regulatory bodies moved to enhance the requirements for providers of professional services throughout the U.S. Although new standards were introduced in a number of areas, few were more specific and impactful than American Bar Association Formal Opinion 483 (2018), which applies to all licensed attorneys.

Given the increasing frequency of cybersecurity threats, the American Bar Association issued Formal Opinion 483 to allow companies to better understand their attorneys' obligations to guard against cyberattacks, to protect the electronic information provided to the attorney, and to respond if an attack occurs. An attorney's failure to adhere to these guidelines could result in damage to their business.

Formal Opinion 483 clarifies the steps attorneys must take to secure client information. Specifically, it says "lawyers must employ reasonable efforts to monitor the technology and office resources connected to the internet, external data sources, and external vendors providing services relating to data and the use of data."

Therefore, the attorney must not only take reasonable steps to ensure that physical copies of client information are protected, but the lawyer must now also take reasonable steps to ensure electronic documents and files are safeguarded.

Formal Opinion 483 also clarifies attorneys' ethical duties to address cyberattacks through proactive incident response plans, investigation and proper notifications. The incident response plan should outline the individual tasked with carrying out each step and the individual responsible for the overall duty to ensure that the incident response plan is undertaken.

In this regard, Formal Opinion 483 states that "a competent lawyer must make all reasonable efforts to restore computer operations to be able again to service the needs of the lawyer's clients."

With respect to the investigation, the attorney must make reasonable attempts to ensure the attack has been stopped and to determine what happened, including whether data was accessed or lost.

Finally, attorneys' notification requirements "will depend on the type of breach that occurs and the nature of the data compromised by the breach." Client notification is required if material client information has been "accessed, disclosed or lost in a breach."

In light of the foregoing, attorneys should take reasonable actions to at least do the following:

- Protect their computer system and ensure their vendors are doing the same.
- Have an incident response plan in place to stop the attack and minimize the damage.
- Conduct an investigation to determine exactly what happened.
- Notify and advise clients as required.

While the duties set forth in Formal Opinion 483 clearly impact the legal profession, they exemplify best practices for all providers of professional services. All professionals would be wise to ensure that they meet certain minimum standards similar to those set forth in this opinion.

5. THE CONTINUED EVOLUTION OF CYBERSECURITY INSURANCE

Do you need cyberliability insurance? The short answer is yes, you do, regardless of the size of your business. Cybercrime is one of the fastest-growing risks to businesses of all sizes. If you have private data that needs protecting, then you are certainly vulnerable. There are many, many examples of companies failing after a cyberevent.

Even more alarming is the fact that 71 percent of all breaches target small businesses, and small-business breaches rose nearly 45 percent within the last two years. Experts believe that weaker and simpler cybersecurity measures make small businesses an easy target for hackers.

While a small business may not have the financial capability to develop and implement cybersecurity measures similar to those used by a larger company, a small business can mitigate the risk and offset the cost of a breach by procuring cyberinsurance.

Cyberinsurance can help cover some of the necessary expenses following a breach, such as the costs of legal and forensic services to determine if and how a breach occurred, notifying impacted customers of the breach, customer credit and fraud monitoring services, and public relations and crisis management fees to help rebuild the company's reputation.

The average cost of a small business data breach is $188,400, up from $73,000 just two years ago. For a large business, this figure can rise into the millions of dollars. While cyberliability insurance will not prevent a breach from occurring, it can help small businesses prevent financial disaster, recover once an incident has occurred, and ensure that all necessary and appropriate response measures are taken.

As is the case with other types of insurance, there is no one-size-fits-all approach to cyberinsurance. Instead, the type of coverage procured, the endorsements and exclusions of the policy, and the deductible and/or self-insured retention amount are a few of the many important considerations a small business must analyze in choosing the cyberinsurance that fits its individual needs.

This article appeared in the December 2018, edition of Westlaw Journal Special Report.

ABOUT THE AUTHORS

Jeffrey M. Dennis (L) is the head of the Privacy & Data Security practice at **Newmeyer & Dillion** in Newport Beach, California. He works with the firm's clients on cyber-related issues, including contractual and insurance opportunities to lessen their risk. He can be reached at Jeff.Dennis@ndlf.com. **Amtoj Randhawa** (R) is an associate in the firm's Privacy & Data Security practice. He focuses on helping clients navigate the legal dispute implications of cybersecurity and advises businesses on implementing and adopting proactive measures to prevent and neutralize threats. He can be reached at Amtoj.Randhawa@ndlf.com.