Cybersecurity law, compliance and protection

By John Bandler, Esq., Bandler Law Firm PLLC

SEPTEMBER 19, 2023

With cybercrime a rampant and expected threat, governments have imposed civil obligations upon organizations to protect themselves and report certain events to authorities and affected parties.

Today, nearly every organization has legal compliance obligations relating to cybersecurity and data breach reporting. The laws can be complicated, and they come from more than one government and agency. A single organization may find itself navigating rules from multiple states and regulators.

Of course, cybercrime — by definition — violates criminal law, and those who commit it are (theoretically) subject to those consequences. Solving the cybercrime problem requires improved enforcement through effective investigation and prosecution ("Solving the Cybercrime Problem," Reuters Legal News, March 21, 2023, https://reut.rs/45Kikmo). Here, we focus on the civil cybersecurity compliance requirements.

Organizations will perceive the threats and obligations differently and will prioritize their work and focus variously. Perhaps there are two extremes to the protection-compliance paradox. Should they focus on preventing cybercrime or on legal compliance? Should they hire an army of cybersecurity experts to lock everything down, or an army of lawyers to interpret and synthesize the various laws and prepare for legal disputes?

Simplifying the complexities

The law surrounding cybersecurity has intricacies that bring attorneys delight. To streamline them we can think about three types of data laws:

- Data breach reporting;
- Cybersecurity;
- Privacy.

Every state has a data breach reporting and notification law, based on the same concept but with varying terminology, definitions, applicability and consequences. Federal regulators also have reporting requirements. Put simply the laws say that if consumer data is accessed improperly, such as through a cybercrime data breach, then the consumers and government need to be notified. These reporting laws were an early step in the evolution of data law, creating a legal obligation to disclose the data breach because otherwise many organizations would remain silent.

This mandated notification after a breach was a start and created some protections and incentives. An obvious next step was to impose a legal duty to secure that data in the first place, which might reduce the number of breaches that occur and require notification.

We know that a step to help prevent our cars from being stolen is to not leave the keys in the car, and not leave it running and unattended. We might not be familiar with the vehicle and traffic laws of some states that suggest not to do this as a measure to reduce theft. Cybersecurity laws follow a similar concept though the complexity is greater.

Have good enough cybersecurity to prevent a data breach. If you prevent the data breach, you are in a good position to prevent a compliance issue.

Most regulators of a particular sector such as finance or health, and a growing number of states, started to impose cybersecurity requirements. Terminology, definitions and specifications vary. Where states have implemented cybersecurity laws they aim to protect state residents, therefore they can apply based on the residence of the consumer rather than the location of the business. This means a business in one state needs to examine its reach and the potential application of other state laws.

A multitude of state cybersecurity laws with national impact can seem complex. But yet they can also be simplified with the standard of "reasonable cybersecurity."

The growing number of state privacy laws are much harder to simplify. Privacy laws will include a cybersecurity and breach notification requirement but also much more; requirements for notice and transparency on what data is collected from the consumer, how that data is used, whether it is shared, rights to correct or delete the data, and other rights.

The California Consumer Privacy Act (CCPA) of 2018 was a major development for privacy law in the country and then was amended by the California Privacy Rights Act (CPRA). Regrettably it is about 25,000 words and it is now supplemented by a regulation, another 25,000 words. If they were an easy read that would mean three hours to navigate through them, but they are not so you should budget more time.

So let us focus on the simpler component of cybersecurity, the threat of cybercrime, and the civil requirements for cybersecurity.

The multiple motivations for cybersecurity

Organizations are made up of people who may focus upon — or ignore — important motivators relating to cybercrime, cybersecurity, and legal compliance.

One motivation is the protection against cybercrime. A realization that cybercrime is a threat that can be costly and damaging. If an organization is not aware of these risks, or believes it will not happen to them, then they will not see the value in protecting against these crimes.

If you experience a data breach, follow required reporting rules and communicate accurately. The government does not take kindly to organizations or individuals who cover up or lie.

Another motivation is legal and regulatory compliance. A belief that regulatory enforcement is a reasonable possibility if cybersecurity is deficient. In highly regulated sectors like finance, organizations know they will be routinely inspected and their information security program reviewed. But in unregulated sectors, some organizations may not even be aware of laws relating to cybersecurity and breach reporting, and enforcement may occur only after a cybersecurity incident that garners sufficient attention.

Compliance is a part of organization management, and good organizations comply with laws and regulations. But compliance should not become a tail that wags the dog, and the compliance function should keep sight on the underlying goals of the legal requirements. Protect from cybercrime.

A third motivation is to advance business needs and revenue. This is the *reason for being* of every organization. Some organizations may view cybersecurity and compliance as cost sinkholes which merely guard against hypothetical risks posed by criminals and government regulators. A more enlightened view puts cybersecurity, cybercrime prevention, compliance and business needs all together. And accepts that effective management of information assets will both protect them and use them to maximum efficiency.

Let's keep it simple

The simple synthesis of the multitude of cybersecurity laws is:

- Have reasonable cybersecurity to protect consumer data.
- If consumer data is breached, notify those people and the government.

For certain regulated sectors, there may be an added requirement to have reasonable cybersecurity to keep the business running safely and soundly.

But legal requirements aside, we can see how all of these should be business imperatives for every organization.

Making compliance simple

Have good enough cybersecurity to prevent a data breach. If you prevent the data breach, you are in a good position to prevent a compliance issue.

If you experience a data breach, follow required reporting rules and communicate accurately. The government does not take kindly to organizations or individuals who cover up or lie.

Synthesizing the laws and action

If the laws require reasonable cybersecurity to protect consumer data, then a sound business will simply expand that zone of protection to the entire business.

Have reasonable cybersecurity to protect all organization data and systems from compromise or impairment. Cyber incidents hurt the business and bottom line in many ways.

Further, a comprehensive view places cybersecurity as a part of overall management of the company, including the information systems. Information assets are essential for every organization. Organizations that manage their data, devices, systems, and information effectively are in a better position to not only prevent harms, but to maximize their efficiency and resources and thus maximize revenue. Legal compliance will flow naturally.

John Bandler is a regular contributing columnist on cybercrime and cybersecurity for Reuters Legal News and Westlaw Today.

About the author

John Bandler is a lawyer, consultant, author, and adjunct professor at Elisabeth Haub School of Law at Pace University. He helps protect organizations from cybercrime, improve cybersecurity, and better manage information assets. His firm, based in New York, is **Bandler Law Firm PLLC**, and he can be reached at JohnBandler@JohnBandler.com.

This article was first published on Reuters Legal News and Westlaw Today on September 19, 2023.