NILES·BARTON&WILMER LLP
Trusted Legal Advisors Since 1838.

NBW's Data Security and Cybersecurity Way: Precise.Preventative.Proactive

DATA SECURITY & CYBERSECURITY LAW

Understanding the Problems, Threats, and Your Legal Responsibility

THE PROBLEMS

HOW FAST ARE THE THREATS?

Cyber threats evolve faster than the government can follow, and the threats are constant.

Every 39 seconds, a device connected to the internet experiences a cyber-attack.

(https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds)

ARE THE DATA SECURITY AND CYBERSECURITY LAWS UNIFORM, AND HOW QUICKLY ARE THE LAWS CHANGING?

The data security and cybersecurity laws vary state by state, country by country, and industry by industry.

Governments are in hyperdrive attempting to keep pace with the threats by adding new and amended laws that place significant liability and immense responsibility on companies.

In the past five years, 38 states added new or amended data security and cybersecurity laws (some, including Maryland, did this multiple times over that period).

DOESN'T MY COMPANY'S EXTERNAL CYBERSECURITY AND/OR IT FIRM KEEP MY COMPANY COMPLIANT REGARDING ALL ASPECTS OF DATA SECURITY AND CYBERSECURITY?

No. External cybersecurity and/or IT firms are not responsible for keeping your company legally compliant with applicable data security and cybersecurity laws.

However, your company is responsible for ensuring they are legally compliant.

THE COSTS

WHY DO HACKERS WANT TO ATTACK MY COMPANY, AND WHAT IS THE ROOT CAUSE OF BREACHES?

Hackers want to steal your client and employee information and data because it is the new currency, and they know that you hold the keys to the vault. Identity theft, financial bank accounts, medical information, irreparable harm.

60% of data breaches come from **mistakes** and **weak links.**

43% of data breaches start with third-party service provider mistakes.

(2018 State of Cybersecurity in Small & Medium Size Businesses, "Ponemon Institute")

DO HACKERS ONLY TARGET LARGE COMPANIES?

No. Small to mid-sized businesses are easier targets.

58% of small to mid-size businesses experienced a cyber attack in 2018.

FINANCIALLY, HOW MUCH DOES A DATA BREACH COST, AND DO PREVENTATIVE MEASURES SAVE MY COMPANY MONEY?

$3.92M is the global average cost of a data breach.

Yes, preventative measures save companies a significant amount of money.

For example, companies that have incident response teams and plans, and test the plans frequently, save, on average, **1.2 million** per data breach.

("Cost of a Data Breach Report 2019," Ponemon Institute)

UNDERSTAND YOUR LEGAL RESPONSIBILITY

WHAT RESPONSIBILITIES DOES MY COMPANY HAVE REGARDING THIRD-PARTY SERVICE PROVIDERS?

In general, companies are responsible for ensuring their third-party service providers are legally compliant with the applicable data security and cybersecurity laws. The law requires companies to include contractual provisions that obligate their third-party service providers to adhere to these laws.

DO THE LOCATION AND SPECIFIC INDUSTRY IMPACT MY COMPANY'S LEGAL RESPONSIBILITIES?

Yes. The applicable law is based on where your company's clients and employees (past and current) live, what information your company has about each, and your company's industry.

WHAT MAKES MY COMPANY LIABLE?

Generally, a company's liability derives from not having the appropriate legally required data security and cybersecurity policies, failing to vet its third-party service providers properly, and, following a data breach, not adhering to the applicable data security notification laws.

WHAT CAN YOU DO?

Prevent and Mitigate through P.A.R. – Prepare. Adapt. Respond.

PREPARE

Develop and Apply.
Craft and implement the appropriate policies and programs that meet the legal requirements of each applicable data security and cybersecurity law and ensure each is followed, effective, and enforced.

Vet, Investigate, and Require.
Ensure that your company's third-party service providers are legally compliant with the applicable data security and cybersecurity laws, and include contractual language that specifies the exact terms for compliance.

Prepare for a Disaster.
Train your company's executives and staff by formal education, cybersecurity workshops, and mock breach simulations and roundtable table exercises to best prevent a data breach and mitigate the potential harms.

ADAPT

Evolve and Confirm.
Review, assess, and revise (as necessary) your company's policies and programs. Ensure that each conforms with any new data security or cybersecurity law.

Evaluate and Assess.
Perform annual evaluations and assessments of your company's third-party service providers, and review and update (as necessary) your contracts with each.

Entrench Security Awareness.
Continue training your company's employees to change the culture around data security and cybersecurity.

RESPOND

Investigate and Analyze.
Determine whether cyberattack meets the legal definition of a data breach.

Notification.
If the cyber-attack does meet the definition of a data breach, follow the specific legal obligations relating to who to notify, what to include in the notification, how to provide notification, and the timing requirements for notification.

Remediate.
Reassess, revise, and rebuild your data security and cybersecurity policies and programs to prevent and mitigate any future harms.