

Cyber Security Summit 2018:

Small & Mid-Size Business Forum

**States Are Making Big Moves on
Data Privacy Laws – What Does
it Mean For You?**

A large, light blue decorative graphic on the left side of the slide, consisting of several overlapping, parallel lines that form a stylized, abstract shape resembling a series of nested chevrons or a stylized letter 'B'.

The past: breach notification

- 10 years ago, states were focused on breach notification
- Slowly, every state caught up and required companies to provide some kind of notice when sensitive information was lost
- This trend was reactive rather than prescriptive



The present: states are getting into the business of regulating how data is held

1. Massachusetts Data Privacy Rule
 - Applies to companies that process, use, maintain or have access to personal information Massachusetts resident.
 - Imposes a requirement to have a security program that meets certain standards.



The present (con't):

2. Nevada

- Applies to any corporation doing business in the state.
- Data collectors that do any business in Nevada must use encryption in certain circumstances.



The present (con't):

3. Alabama

- Businesses must protect “sensitive personally identifying information.”
- The statute defines what may constitute reasonable security measures.
- Must designate an employee, do risk assessment, contract with vendors, keep management informed.



The present (con't):

4. Colorado

- Sept 1, 2018: 30-day notification.
- Companies must maintain written procedures for disposing of data and take "reasonable" steps to protect the personal data that they have and that they share.
- PI includes combinations of usernames and email addresses with passwords or security codes.



The present (con't):

5. Nebraska

- Must implement and maintain reasonable security procedures and practices to secure that data.
- Must ensure that any third-party vendors that have access to the PI contractually agree to implement appropriate security procedures and practices to protect that information.
- The failure to comply with LB757 can subject the company to enforcement by the Nebraska Attorney General.



THE FUTURE: EXPANDING AND MOVING TOWARDS THE EUROPEAN MODEL

California Consumer Privacy Act (CCPA) – takes effect January 1, 2020


- “Mini GDPR.”
- Reaches many consumer facing companies.
- New concept of what is sensitive information.
- Companies must “implement and maintain reasonable security procedures and practices appropriate to the nature of the information.”
- Enforcement actions and possible class action lawsuits.



How do you respond to these big moves?

Take reasonable steps, including:

- Have a data security program and follow your policies.
- Assign someone the job and give them authority.
- Annual risk assessment/evaluation of policies.

- 
- A decorative graphic in the top-left corner consisting of several overlapping, light blue chevron-like shapes pointing to the right.
- Do the basics.
 - Train your employees.
 - Establish relationships with vendors and a cyber security lawyer.

- Take incident response seriously.
- Invest.



QUESTIONS?



**Phil Schenkenberg J.D., CIPP/US
Cyber Attorney, Shareholder**

pschenkenberg@briggs.com
<https://www.linkedin.com/in/philschenkenberg>



**Cyrus Malek J.D.
Cyber Attorney, Associate
Certification in Cybersecurity and Privacy Law**

cmalek@briggs.com
<https://www.linkedin.com/in/cyrus-malek-86631b4>



**The Privacy, Data Security and Cybersecurity practice group
at**

**Briggs and Morgan offers a full range of services to help
clients prevent, prepare for, and minimize the impacts of
data security breaches and cyber attacks. We also represent
clients in litigation following data breaches.**