Cyber CYA Webinar Series:

Privacy & Cyber Integration, Legislation Enforcement

Colorado SBDC TECHSOURCE

CYBER: Cover Your Assets™

THE PIKES PEAK SMALL BUSINESS DEVELOPMENT CENTER HAS BEEN DEDICATED TO HELPING EXISTING AND NEW BUSINESSES GROW AND PROSPER FOR MORE THAN 30 YEARS.

FREE CONSULTING

PRACTICAL TRAINING

BUSINESS RESOURCES

El Paso County Colorado

Ent Business Banking

Colorado Springs Olympic City USA

PSBTrust.com Park State Bank & Trust

CenturyLink

VectraBank Colorado

Powered by SBA U.S. Small Business Administration

Funded in part through a cooperative agreement with the U.S. Small Business Administration

WWW.PIKESPEAKSBDC.ORG/CONSULTING

WWW.PIKESPEAKSBDC.ORG/WORKSHOPS

CYBER CYA: Privacy & Cyber Integration, Legislation Enforcement

Agenda:

The road to Regulation

What will it cover?

California - Data Security Breach Reporting

Colorado's New Privacy and Cybersecurity Law

Is GDPR The Future of Global Data Privacy Laws?

Financial and Operational Realities

Why does this matter to you?

What can you do as a small business?

Presented by: Dr. Shawn P. Murray, C|CISO, CISSP, CRISC
Murray Security Services
SBDC Consultant

Privacy & Cyber Security

Many businesses process, transmit or store information or data that qualifies as personal identifiable information, otherwise known as PII. Many laws articulate what qualifies as PII in the United States. HIPAA, FERPA, PCI-DSS, Privacy Act of 1974 are just a few of the most common laws and standards that require protection of PII.

Some laws have specific criteria as to what qualifies as PII and identify protection requirements as well as reporting requirements if PII is breached or stolen.

This webinar will cover the basic requirements for appropriate identification and protection of employee and customer data as well as specific Colorado regulatory requirements when dealing with breaches not covered by federal laws. We will also discuss complex enforcement requirements.

The presenter will provide examples of breaches to help organizations identify business processes that may increase risk and recommend solutions to reduce them.

Colorado SBDC TECHSOURCE
CYBER: Cover Your Assets

THE ROAD TO REGULATION

UNITED NATIONS
UNCTAD

- According to a new, interactive map by the United Nations Conference on Trade and Development (UNCTAD)
  - 58 percent of the 194 UNCTAD member countries report having data protection and/or privacy legislation on the books and
  - 10 percent have draft legislation in the works.
  - Unfortunately, 21 percent of countries have no legislation or anything in process.

THE ROAD TO REGULATION

UNITED NATIONS
UNCTAD

- A global map of cyberlaws, the **Global Cyberlaw Tracker** monitors the state of e-commerce legislation including laws over e-transactions, consumer protection, data protection/privacy, and cybercrime.
- It's a helpful tool for organizations as they work to safeguard the personal information of citizens around the globe.
- However, it's also a good illustration of the significant challenge organizations face in data protection compliance.

THE ROAD TO REGULATION

- To further complicate matters for the companies that do business with Americans, ***there is no federal data privacy law in the United States***.
- Instead, companies are left to interpret and comply with a growing patchwork of individual state laws — a movement now gaining momentum thanks to the California Consumer Privacy Act (CCPA) of 2018.
- The following states have developed significant cyber security & Privacy laws as well.
  - Colorado
  - New York
  - Vermont
  - Massachusetts

California - Data Security Breach Reporting

California law requires a business or state agency to notify any California resident whose unencrypted personal information, as defined, was acquired, or reasonably believed to have been acquired, by an unauthorized person. (California Civil Code s. 1798.29(a) [agency] and California Civ. Code s. 1798.82(a)[person or business])

Any person or business that is required to issue a security breach notification to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General. (California Civil Code s. 1798.29(e) [agency] and California Civ. Code s. 1798.82(f)[person or business])

Note: This form is only for use by businesses and state and local government agencies, which are required to submit a sample notice if they experience a breach of personal information involving more than 500 California residents.

The California Consumer Privacy Act of 2018

A bill passed by the state of California legislature and signed by its governor on June 28, 2018.

Beginning Jan. 1, 2020, the bill, in part, will grant a consumer the right to request a business to disclose the categories and specific pieces of personal information that it collects about the consumer, the categories of sources from which that information is collected, the business purposes for collecting or selling the information and the categories of third parties with which the information is shared.

The bill would also require a business to make disclosures about the information and the purposes for which it is used.

The purpose of this article is to introduce marketers to the major concepts of the new California Consumer Privacy Act of 2018 (CCPA).

In future coverage, California will provide action steps on how marketers can begin to prepare for these changes that affect any company that collects data of private Californian citizens.

The California Consumer Privacy Act of 2018

To Whom Does the Law Apply?

Businesses that meet the following thresholds are liable for compliance with the California Consumer Privacy Act of 2018:

- Has annual gross revenues in excess of $25 million
- Annually buys, receives for the business' commercial purposes, sells or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households or devices
- Derives 50 percent or more of its annual revenues from selling consumers' personal information.

Colorado Passes Far Reaching New Privacy & Cybersecurity Law

(House Bill 18-1128)

- Recently, a new bill was signed by former Colorado Governor John Hickenlooper, creating far reaching new requirements for entities that collect or maintain personal identifying information of Colorado residents.
- These requirements, has created one of the strictest state-based privacy and data breach laws in the country, went into effect September 1, 2018. The Colorado Attorney General's office led part of the effort to pass the new law, making enforcement a likely priority.
- The new law requires organizations to maintain a policy for disposing documents with consumer data and notify Colorado residents of any potential personal information exposure no later than 30 days after discovering a data breach.

The 30-day notification window does not provide for any specific exemptions (such as HIPAA) and is the shortest of any U.S. state.

Colorado SBDC TECHSOURCE
CYBER: Cover Your Assets

Colorado Passes Far Reaching New Privacy and Cybersecurity Law (House Bill 18-1128)

1. Why are lawyers calling the new Colorado Privacy law "Landmark"?

The new Colorado Privacy and Cybersecurity law, officially known as H.B. 18-1128 and which took effect on Sep. 1, 2018, is a major change to Colorado's privacy law. All companies who do business in Colorado and that handle personally identifiable information (PII) are required to comply. There is no exemption for small businesses. This is a very unusual situation.

2. What are the basic requirements of the law?

Businesses must implement and maintain reasonable security measures to protect documents containing personally identifiable information, both on paper and electronically. They must ***contractually*** require third parties that they share this data with, such as cloud service providers and other vendors, to implement those same reasonable security measures and they must implement a written policy covering the disposal of documents containing PII. In addition, the definition of PII in this law is extremely broad. Finally, businesses who have a data breach must notify the parties affected within 30 days with no extensions. This is the toughest notification provision in the country.

3. What is the definition of reasonable?

Conveniently, the law doesn't define that, but they do say that it should be commensurate with the risk. Ultimately, if the Attorney General asks, you need to be able to convince her that what you have done is reasonable. It is our opinion that "reasonable" means "best practices" and those have become pretty clear for cybersecurity (see below). Our current AG was very involved in the crafting of this bill, so assume that she has a strong opinion of what is reasonable. The definition of reasonable will be adjusted as a result of the lawsuits that the AG files over the next couple of years.

Colorado Passes Far Reaching New Privacy and Cybersecurity Law (House Bill 18-1128)

4. What are the consequences of not complying?

The Attorney General can sue for non-compliance and also to recover damages to Colorado residents. More significantly, the AG can file criminal charges if requested by any local District Attorney or the Governor.

5. What are the key components of a company's reasonable security program?

Again, thinking in terms of "best practices," some of the key components of a reasonable security program include:

- Create and implement a written information security program
- Perform a risk assessment annually
- Implement ongoing employee training
- Encrypt data at rest
- Implement a set of security policies and procedures
- Create a disaster recovery program
- Implement an incident response program
- Create a document/data retention and disposal policy
- Implement a third party/vendor cyber risk management program.

IS GDPR THE FUTURE OF GLOBAL DATA PRIVACY LAWS?

- To avoid having to comply with 50 different state laws, big tech companies are calling for a unified law similar to the European Union's GDPR, though more so in concept than in scope.
- Most data privacy activists champion the regulation, however many organizations are cautious about what they ask for.
- GDPR is considered the world's most stringent data protection law. Since going into effect in May of last year, nearly 60,000 data breaches have been reported but only 91 fines have been imposed to-date.
- According to one report by international law firm DLA Piper, the three biggest offenders so far are the Netherlands, Germany, and the United Kingdom.

The GDPR (General Data Protection Regulation)

Effective May2 5, 2018

Seeks to create a harmonized data protection law framework across the EU and aims to give back to data subjects, control of their personal data, whilst imposing strict rules on those hosting and processing this data, anywhere in the world.

- GDPR is designed to give individuals better control over their personal data and establish one single set of data protection rules across Europe.
- Organizations outside the EU are subject to this regulation when they collect data concerning any EU citizens . 50% of global companies say they will struggle to meet the rules set out by Europe unless they make significant changes to how they operate, and this may lead many companies to appoint a Data Protection Officer.

The GDPR (General Data Protection Regulation)

Effective May2 5, 2018

- Personal data is defined as any information relating to an identified or identifiable natural person.
- This includes online identifiers, such as IP addresses and cookies if they are capable of being linked back to the data subject.
- This also includes indirect information, which might include physical, physiological, genetic, mental, economic, cultural or social identities that can be traced back to a specific individual.
- There is no distinction between personal data about an individual in their private, public, or work roles – all are covered by this regulation

The GDPR (General Data Protection Regulation)

Effective May25, 2018

Questions to Consider

1. Does senior management or the business owner understand the importance of GDPR?
2. Do you know where your data is today?
3. Do you have a process to provide data to individuals who ask?
4. Do you have a process to delete data if demanded?
5. Do you understand the consent rules?
6. Do you follow privacy by design and privacy by default principles when designing new systems?
7. Do you know which outsourcers have access to the data?
8. Are you sure you can detect data breaches?
9. Do you have a communication plan ready to go after a data breach?
10. Have all processes and data flows been documented?

Colorado SBDC TECHSOURCE
CYBER: Cover Your Assets

Why does this matter to you?

- Keeping up with the evolving regulatory landscape requires constant attention – just like monitoring sensitive data that is always on the move.
- While the world's lawmakers scramble to keep up with escalating data privacy issues, costly fines and the court of public opinion is already underway.
- It's important to understand what data you collect, where it's shared, and how it's protected.
- While many data privacy regulations are still being developed, implementing measures to align with larger privacy frameworks like **GDPR** can ensure your organization's data is protected and you're prepared for forthcoming regulations.

What can you do as a small business?

- ✓ Categorize and classify your information
  - Develop an information and data classification scheme
- ✓ Categorize and classify your systems
  - Align the scheme above to the systems you use to process transmit & store sensitive data
- ✓ Perform an inventory
  - See what laws apply to your business processes
- ✓ Develop a plan
  - Determine what applies to your organization
- ✓ Talk to an SBDC Consultant
  - Make an appointment to get assistance!

Colorado SBDC
PIKES PEAK Small Business Development Center

QUESTIONS?

References & Resources

https://www.mintz.com/insights-center/viewpoints/2018-06-colorado-passes-far-reaching-new-privacy-and-cybersecurity-law

https://oag.ca.gov/privacy/databreach/reporting

https://www.bfaslaw.com/2017/08/08/cybersecurity-and-californias-breach-notification-law/

https://www.caprivacy.org/

https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

https://studentprivacy.ed.gov/sites/default/files/resource_document/file/checklist_data_breach_response_092012_0.pdf

https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=IMM14202GBEN

https://www.skyhighnetworks.com/cloud-security-blog/top-10-questions-to-test-your-gdpr-readiness/

https://www.dizzion.com/resource/blog/5-things-companies-should-know-about-colorados-new-privacy-law/

Pikes Peak Small Business Development Center

559 E. Pikes Peak Ave., Suite 101, Colorado Springs, CO 80903

719-667-3803
sbdc@elpasoco.com

www.pikespeaksbdc.org

OUR SPONSORS:

Funded in part through a cooperative agreement with the U.S. Small Business Administration