INSIGHTS FOR SMALL BUSINESSES
CYBERSECURITY & DATA PRIVACY

Cybersecurity and data privacy are similar but different. There are different agencies and laws that regulate different types of incidents, oftent with overlapping interests.

Cybersecurity: Protection of networks and infrastructure from attacks and breaches.

Data Privacy: Protection of a person's "personal identifiable information" from being accessed and/or acquired.

It is important to pay attention to the cybersecurity and data privacy risks within your company because the risk of loss extends to almost everyone who does business. On top of that, your company may be legally responsible for data breaches that occur as a result of even a vendor or by an acquired company. The consequences outweigh non-action.

By 2025, cybercrime costs are expected to exceed this annually.	**$10.5 T**
During the 2020 pandemic, ransomware and phishing attacks increased this much.	**715 %**
Of data breaches over the past two years occurred with small and medium-sized businesses.	**60%+**

ENFORCEMENT

Each state currently has its own method of enforcement. Generally speaking, most states have some form of state comprehensive privacy law introduced or in review, while a few have signed these laws into practice.

When companies tell consumers they will safeguard their personal information, the FTC can and does take law enforcement action to make sure that companies live up these promises. The FTC has brought legal actions against organizations that have violated consumers' privacy rights, misled them by failing to maintain security for sensitive consumer information, or caused substantial consumer injury. In many of these cases, the FTC has charged the defendants with violating Section 5 of the FTC Act, which bars unfair and deceptive acts and practices in or affecting commerce. In addition to the FTC Act, the agency also enforces other federal laws relating to consumers' privacy and security.

INCIDENT RESPONSE PLANS

It is essential that your organiztion setup an incident response plan. There are many different items that must be thought out ahead of time to ensure you are covered in the case of a breach. Where you do business and where your business is located can also affect what should be included.

Just because you have a plan too doesn't mean you are covered. There are regular maintenance items that must be done such as regular employee training and regular audits and testing. Some of the current laws require yearly security training to be necessary to ensure "reasonable" security and privacy protections.

CYBER INSURANCE

For some businesses it can make sense to invest in cyber insurance. There are different types of cyber insurance you can purchase depending on your business's risk.

- **Network Security & Privacy Liability** – coverage for defense costs, damages, and expenses arising from theft or improper disclosure of confidential information
- **Extortion/Ransomware** – coverage for costs associated with lost income and extortion demands
- **Data Breach Response** – costs incurred with responding to data breach (i.e., CCPA)
- **Business Interruption/Data Restoration**

The costs associated will depend on a multitude of factors such as the strength of security measures, evolution of laws, types of claims covered or excluded, and the amount and sensitivity of data covered.

CONCLUSION

Taking proactive measures to protect your data and ensure you have adequate cybersecurity measures set up is essential. Contact us today if you have any questions or need any support in ensuring your business is protected.

BROOKS KUSHMAN
INTELLECTUAL PROPERTY AND TECHNOLOGY LAW