Looking Ahead by Reflecting on the Year Past:

How to Prepare for the Emerging Cybersecurity Landscape in 2019

The past year was marked by headline-grabbing data breaches, significant data privacy and security legislation, and increased litigation and government investigation into companies' information security practices. Companies would be better equipped to face the challenges of the year ahead if they take heed of the lessons of the year past.

Anna Mercado Clark, CIPP/E
Partner

Recently, the second-largest data breach (by number of affected consumers) was disclosed by a hospitality company. What are some takeaways from the history-making data breaches of 2018?

Even Traditionally Non-Consumer Facing Companies Are Targets

It is a misconception that bad actors are interested in only financial information. Confidential business information, intellectual property, and even confidential health or tracking information are similarly valuable to bad actors. Increasingly, bad actors are not only accessing information, but they are also launching denial-of-service attacks that can cripple business operations.

Accordingly, while companies in the banking, health care, hospitality, retail and insurance industries continue to be targets, traditionally non-consumer facing companies are also increasingly being targeted. These include companies in the manufacturing, construction, legal and energy industries, as well as educational institutions and media companies. Your legal counsel should be familiar with your particular industry's needs and any applicable regulatory framework.

Preparation Is Key

In addition to incident response preparedness, policies regarding data management and recovery may mitigate risks and the business impact of a breach (including those caused by human error, a cyberattack or a disloyal employee). Legal counsel with actual experience with incident and post-incident response management can provide forward-thinking pre-incident advice regarding these issues.

Legal advice regarding the nuances of cyber (and other related) insurance policies prior to purchase can assist in a company's selection process and identify coverage gaps. Seek advisors with technical competency. Counsel should be at the forefront of technological developments, including artificial intelligence, that may increase risk or provide new defensive solutions. Certain privacy and technical certifications may be helpful in vetting a legal team's knowledge and experience.

Think Beyond Your Own Data or Organization

An organization is only as protected as the weakest link in its supply chain. Bad actors often target organizations through their smaller or inconspicuous vendors, contractors or even subcontractors. Implementing a comprehensive vendor risk management and contracting system, assisted by experienced legal counsel, can mitigate this risk.

Companies holding data for another organization should be aware of the attendant risks and obligations regarding that data. Information security risks should be examined and risk allocation negotiated in transactions involving mergers and acquisitions.

There have been many legislative and regulatory developments in and outside of the United States in the past year. What are some of the most impactful?

- As of this year, all 50 states, as well as the District of Columbia, Guam, Puerto Rico and the U.S. Virgin Islands, have data breach notification laws on the books.
- To date, over 20 states have additional laws that require certain security practices to protect their residents' personal information from unauthorized access, disclosure, modification or loss. These include the New York State Department of Financial Services (NYSDFS) Cybersecurity Regulation and the California Consumer Privacy Act of 2018 (effective in 2020). These laws may apply to companies that license, use, collect or store information from residents in those states, even if the companies are located elsewhere. Additional, industry-specific regulatory requirements may also apply.
- The European Economic Area's General Data Protection Regulation (GDPR) took effect and enforcement actions (including against American and Canadian companies) have begun. Other countries are enacting legislation that track the GDPR, and the United States is likely to consider a unified, national data privacy and security law in the coming year.

Legal counsel should be equipped to provide guidance on all laws that may apply to your business (and identify all those that do not). Even companies that operate solely in one state may be subject to other states' or countries' laws.

In sum, here are our proposed 2019 cyber-security resolutions:

- Prepare by implementing sound internal policies vetted by experienced legal counsel.
- Reduce risk by implementing a comprehensive vendor risk management and contracting system.
- Seek legal counsel before purchasing cyber insurance to identify coverage gaps.
- Select legal counsel with experience in your particular industry and the applicable laws and regulations.

Companies can, and should, prepare for the challenges ahead. Legal counsel who understand a company's specific needs, resource limitations and industry can be invaluable in doing so.

Anna Mercado Clark, CIPP/E is a partner at Phillips Lytle LLP and leader of the firm's Data Security & Privacy and E-Discovery & Digital Forensics Practice Teams. She can be reached at aclark@phillipslytle.com or (716) 847-8400, ext. 6466.