POLSINELLI

in the news

Commercial Litigation

February 2014

Cyber Security: Are You at Risk?

by: G. Gabriel Zorogastua

In this Issue:

As the recent Target and Neiman Marcus data breaches made clear, cyber security is one of the top threats to business today. These threats can be devastating to companies - damaging customer confidence, the company brand, and the bottom line by increasing costs through remediation costs, lost revenues and customers, litigation, and fines. Governments and customers are now holding businesses accountable for inadequate protection of customer data. Cyber security concerns are now part of doing business, and general counsel and executives should be ready to guide their companies through these complex issues.

Prevention

Prevention is the best ways to minimize cyber-security liability. The following steps can minimize the cost and likelihood of security breaches:

- Security measures before a breach. Studies have found that having an incident response plan, establishing a strong security infrastructure, and appointing a Chief Information Security Officer can lower the costs of a data breach by approximately 50%.

- Cyber-security audits. Businesses should conduct regular cyber-security audits and limit the access of sensitive data by third parties and employees.

- Cyber-security insurance. Businesses should review insurance policies to determine whether and to what extent they are covered for cyber-security threats.

- Encryption. If a data breach occurs, encryption can help minimize liability.

Notification

If a data breach occurs, businesses must immediately determine whether they have notification obligations under federal or state law. Congress has yet to enact comprehensive federal law governing notification in the private sector, so businesses must conduct a state- and industry-specific analysis. The following are examples of notification obligations:

- Health Insurance Portability and Accountability Act and Health Information Technology for Economic and Clinical Health Act. HIPAA requires covered entities to protect against reasonably anticipated threats or hazards to security. The HITECH Act requires covered entities and business associates to notify the individuals whose protected health information was accessed no later than 60 days after the breach was discovered. If the breach affects more than 500 individuals, the law also requires notification within 60 days after the breach was discovered to the US Department of Health and Human Services and the media.

- Gramm-Leach-Bliley Act. This act requires financial institutions to publicize their privacy policies and establish internal safeguards and procedures to protect customer information. Related guidelines require covered financial institutions to notify customers whose personal information has been subject to unauthorized access or use if misuse of the customer's information has occurred or is reasonably possible, unless law enforcement determines that notification will interfere with a criminal investigation.

- Securities & Exchange Commission. The SEC has issued guidance stating that publicly traded companies should report certain instances of cyber incidents.

- State law. Currently, 46 states, the District of Columbia, Puerto Rico, and the Virgin Islands have enacted laws requiring notification of security breaches involving personal information.

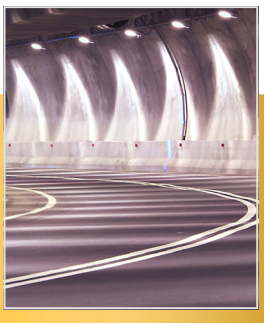
Potential Litigation

Businesses should be ready for litigation if a data breach occurs. Potential claims by private parties and the government include:

- State-law claims. Businesses could face suits under individual states' consumer protection laws, tort and contract law, fiduciary requirements, and other cyber security rules.

- FTC Safeguards Rule. The FTC has brought numerous enforcement actions to address whether businesses security systems are reasonable and appropriate to protect consumer information.

- SEC Enforcement Actions. The SEC's Division of Corporation Finance has taken the position that public companies should disclose their risk of cyber incidents. Failure to disclose cyber security breaches or risks could lead to actions on security anti-fraud provisions like Rule 10b-5 or books and records violations under Rule 13b2-2.



Conclusion

A business's cyber-security obligations are too complex and industry-specific to outline in a short e-blast. Regardless, it is critical for businesses to be prepared. We recommend that businesses, at a minimum, review, update, and implement their cyber security policies, train executives, and promptly investigate potential security breaches. Polsinelli's litigation team and its dedicated cyber security attorneys are ready to help clients lower their cyber-security risks, analyze their obligations, and minimize litigation exposure should a breach occur.

For More Information

If you have specific questions related to this Alert, please contact:

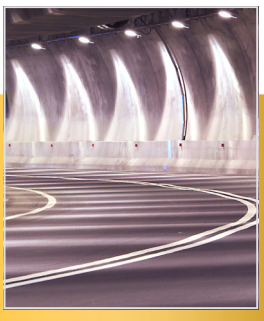
- G. Gabriel Zorogastua | *Author* | 816.374.0537 | gzorogastua@polsinelli.com
- Russell S. Jones Jr. | *Practice Area Chair* | 816.374.0532 | rjones@polsinelli.com
- S. Jay Dobbs | *Practice Area Vice Chair* | 314.552.6847 | jdobbs@polsinelli.com
- Stacy A. Carpenter | *Practice Area Vice Chair* | 303.583.8237 | scarpenter@polsinelli.com
- Tim D. Steffens | 816.572.4595 | tsteffens@polsinelli.com
- Gregory M. Kratofil | 816.360.4363 | gkratofil@polsinelli.com

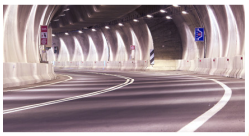
To contact another member of our Commercial Litigation law team, click here or visit our website at www.polsinelli.com > Services > Commercial Litigation > Related Professionals.

To learn more about our Commercial Litigation practice, click here or visit our website at www.polsinelli.com > Services > Commercial Litigation.

To contact another member of our Technology Services law team, click here or visit our website at www.polsinelli.com > Services > Technology Services > Related Professionals.

To learn more about our Technology Services practice, click here or visit our website at www.polsinelli.com > Services > Technology Services.





About Polsinelli

real challenges. real answers.[SM]

Serving corporations, institutions, entrepreneurs, and individuals, our attorneys build enduring relationships by providing legal counsel informed by business insight to help clients achieve their objectives. This commitment to understanding our clients' businesses has helped us become the fastest growing law firm in the U.S. for the past five years, according to the leading legal business and law firm publication, *The American Lawyer.* With more than 700 attorneys in 18 cities, we work with clients nationally to address the challenges of their roles in health care, financial services, real estate, life sciences and technology, energy and business litigation.

The firm can be found online at www.polsinelli.com.

Polsinelli PC. In California, Polsinelli LLP.

About this Publication

If you know of anyone who you believe would like to receive our e-mail updates, or if you would like to be removed from our e-distribution list, please contact Kim Auther via e-mail at KAuther@polsinelli.com.

Polsinelli provides this material for informational purposes only. The material provided herein is general and is not intended to be legal advice. Nothing herein should be relied upon or used without consulting a lawyer to consider your specific circumstances, possible changes to applicable laws, rules and regulations and other legal issues. Receipt of this material does not establish an attorney-client relationship.

Polsinelli is very proud of the results we obtain for our clients, but you should know that past results do not guarantee future results; that every case is different and must be judged on its own merits; and that the choice of a lawyer is an important decision and should not be based solely upon advertisements.

Polsinelli PC. In California, Polsinelli LLP.