—Reprinted with permission from PIA Management Services Inc.—

CHRIS MEYER, ESQ.
Attorney, Whiteman Osterman and Hanna

How N.Y.'s cybersecurity regulations affect you

New York's "first-in-the-nation" cybersecurity rules are now a reality. For PIA agencies, these new regulations represent both a challenge and an opportunity. While the new regulations impose additional burdens and costs on PIA agents operating in New York, agents who proactively address this challenge can reduce their legal exposure and seize new business opportunities.

Reasons for the regulations

Cybersecurity risks have been known for years. The first computer viruses began circulating in the 1970s and by the 1980s, Hollywood was making movies about high school kids almost starting World War III by hacking into NORAD (remember, *War Games*?). Since then, real-world, high-profile attacks have multiplied in number and effect. The Target and Home Depot data breaches cost those companies more than $500 million.[1] Other recent high-profile attacks, including the 2014 Sony breach, have cost millions more.[2]

Despite these significant costs, which do not account for uncompensated losses suffered by consumers and business partners, companies' cybersecurity spending continues to lag behind the growing cost of cybercrime. While Gartner estimates that annual worldwide cybersecurity spending will more than double from $75 billion in 2015 to $170 billion in 2020, the cost of cybercrime is expected to quadruple over that same time period from approximately $500 billion in 2015 to more than $2 trillion by 2019.[3]

In issuing its new cybersecurity regulations, the New York Department of Financial Services described what it sees as the continuing disconnect between cybersecurity spending and cyberthreats. While the NYDFS recognized that "many firms have proactively increased their cybersecurity programs with great success,"[4] it moved forward with the new regulations to encourage all "regulated institutions that have not done so to move swiftly and urgently to adopt a cybersecurity program and for all regulated entities to be subject to minimum standards with respect to their programs."[5]

Legal impact of the regulations

The NYDFS regulations are detailed and will require significant time and resources for PIA agencies operating in New York—large and small—to comply. PIA agencies are strongly encouraged to review the new regulations; monitor ongoing guidance provided by PIA; and consult with their IT providers, privacy professionals, and legal counsel to determine what additional steps they should take.

As agencies work to comply with the new regulations, two critical provisions should be understood. First, the new regulations do not allow agencies to simply delegate responsibility for cybersecurity compliance to IT providers. Second, because cyberthreats are constantly evolving, the new regulations will require ongoing compliance efforts.

For most PIA agencies, hiring a full-time, dedicated IT Department may not be a financial possibility. The NYDFS regulations take this into account by allowing agencies to hire a third party to implement and maintain their cybersecurity program. The regulations, however, require agencies to maintain ongoing supervision of the IT provider by "designating a senior member of the Covered Entity's personnel responsible for direction and oversight of the Third Party Service Provider."[6] In addition, the regulations require a board member or senior officer to certify each year that an agency is in compliance with the regulations.[7]

The new regulations also require active and ongoing evaluation of all agencies' cybersecurity programs through a periodic "risk assessment."[8] This periodic risk assessment must be "updated as reasonably necessary

to address changes" to information systems, nonpublic information held by an agency and changes in business operations.[9]

The combination of senior management responsibility and the requirement to regularly update each agency's cybersecurity program, means that cybersecurity cannot be treated as an out-of-sight, out-of-mind issue to be addressed and forgotten. To protect themselves, agencies should treat cybersecurity as core business function.

Although the NYDFS has not provided any specific guidance on the penalties that may issue for violations, the regulations make clear that all penalties available pursuant to the department's regulatory power are available.[10] As an example of how seriously data breaches are treated by other regulators, the federal Department of Health and Human Services recently levied fines of $475,000 and $2.2 million in separate data breach cases.[11]

Opportunities for proactive agents

PIA agencies handle extremely valuable, sensitive personal information of customers on a daily basis, including Social Security numbers, bank account numbers, health records and other highly personal information. Customers expect businesses to protect their sensitive information and are making purchasing decisions based on companies' privacy and cybersecurity practices.

Recently, the research firm IDC conducted a poll that found 84 percent of U.S. consumers are concerned about the privacy of their personal information.[12] IDC also reported that 78 percent of those polled responded that they would switch to another business if they were directly affected by a data breach. This research suggests not only that protection of customer information is important to maintaining your current customer relationships, but also can be a significant driver of new business opportunities.

PIA agencies should strongly consider using the new NYDFS regulations as an opportunity to demonstrate to clients that you are taking steps to protect their sensitive and confidential information. This can be an especially useful competitive differentiator for PIA agencies that also operate outside of New York, where state-level cybersecurity regulations may not yet have been adopted.

Conclusion

Business owners rarely welcome new regulations. However, in this

case agencies that proactively move to comply with the regulations will have the opportunity to achieve greater security and, hopefully, win new business that will offset the cost of compliance.

Meyer is an attorney with Whiteman Osterman and Hanna in Albany, N.Y. His practice includes corporate and litigation matters, including matters involving cybersecurity, privacy, commercial disputes and labor and employment. He also has been certified by the International Association of Privacy Professionals as an Information Privacy Professional (CIPP/US).

[EDITOR'S NOTE: To help professional, independent agencies comply with the NYDFS' cybersecurity regulations, PIA Management Services Inc., has partnered with Albany-based TAG Solutions to offer a risk assessment and cybersecurity program. See the PIA website (pia.org) for more information.]

[1] *Jim Daly, Expenses from the Home Depot and Target Breaches Surpass $500 Million,* Digital Transactions, *May 26, 2016*

[2] *Robert Hackett, How Much Do Data Breaches Cost Big Companies? Shockingly Little,* Fortune, *March 27, 2015*

[3] *Steve Morgan, Worldwide Cybersecurity Spending Increasing to $170 Billion by 2020,* Forbes.com, *March 9, 2016; Steve Morgan, Cybersecurity Spending Outlook: $1 Trillion from 2017 to 2021,* CSO, *Jun. 15, 2016*

[4] *New York Department of Financial Services, Proposed 23 NYCRR 500, Cybersecurity Requirements for Financial Services Companies ("NYDFS Cybersecurity Regulations"), Section 500.00: Introduction, Dec. 28, 2016*

[5] *Id.*

[6] *NYDFS Cybersecurity Regulations, Section 500.04(a)(2)*

[7] *Id. at Section 500.17(b)*

[8] *Id. at Section 500.09(a)*

[9] *Id.*

[10] *Id. at Section 500.20*

[11] *Office of Civil Rights, Department of Health and Human Services, Press Release, First HIPAA Enforcement Action for Lack of Timely Breach Notification Settles for $475,000, Jan. 9, 2017; Office of Civil Rights, Department of Health and Human Services, Press Release, HIPAA Settlement Demonstrates Importance of Implementing Safeguards for ePHI, Jan. 18, 2017*

[12] *Matt Hamblen, Privacy Worries Are on the Rise, New Poll of U.S. Consumers Shows,* Computerworld, *Jan. 30, 2017*