BY JIM WRYNN and ANTHONY J. FERRANTE

What Insurance Companies Need to Know About Part 500 Cybersecurity Compliance

If there were any remaining doubts about the vulnerability of our online systems, they were dispelled in September when giant credit-reporting company Equifax revealed it was breached in July by cybercriminals, compromising the personal identifiable information (PII) of roughly 143 million Americans – approximately half the country.

With PII – Social Security and bank account numbers; passport and health-related information; driver license and student information – criminals can apply for loans and credit cards, withdraw money from bank accounts, and fraudulently obtain a variety of goods and services. And these criminals know insurance companies store large volumes of PII on their policyholders, making the insurance sector a prime target for cyber crooks.

For example, Anthem Blue Cross Blue Shield and Premera Blue Cross suffered data breaches in 2015 that exposed the PII of approximately 78 million policyholders and cost those companies hundreds of millions in remediation costs. In June 2017, Anthem agreed to pay $115 million to settle lawsuits arising from the breach. However, the total cost Anthem incurred was over triple that amount and included $230 million for costs associated with incident response and $128 million on post-incident cybersecurity enhancements.

The threats to insurers, and all organizations, are growing due to the increasing reliance of business activity on global Internet connectivity, as well as the commercialization and professionalization of cybercrime. This potent combination is driving the increased frequency and severity of cyber incidents. Accordingly, in late 2014, the National Association of Insurance Commissioners (NAIC) Executive (EX) Committee established the Cybersecurity Working Group to create a regulatory framework for cybersecurity. At about the same time, New York's Department of Financial Services (NYDFS) began the process of drawing up its own cybersecurity regulations for the financial services industry, and took effect in March 2017. These regulations are Part 500 of Title 23 of the Official Compilation of Codes, Rules and Regulations of the State of New York, and all financial services organizations licensed, registered, chartered, or otherwise authorized in New York must comply. And it has become clear that the NAIC will incorporate many provisions of the New York regulations into its own framework.

Part 500, designed "to promote the protection of customer information as well as the information technology systems of regulated entities,"[i] requires all companies covered by the regulation to conduct a rigorous assessment of their information systems and risk profiles, and to design and maintain cybersecurity programs commensurate with their risks. Although some companies (including but not limited to those with fewer than 10 employees, less than $5 million in gross annual revenue and less than $10 million in year-end total assets) are exempt from some of Part 500's provisions,

all companies are required to have robust cybersecurity programs and policies in place protecting technology systems and "non-public information"[ii] (which includes PII) that, if disclosed, could cause material harm to any individual, business or either entity's operations. And all companies, no matter their size, are required to ensure the security of information held by or accessible to the third-party service providers they engage.

More specifically, and in addition to the above, Part 500 proposes that institutions:

- Appoint a Chief Information Security Officer (CISO) who, among other duties, will be responsible for achieving compliance with Part 500;
- Deploy key technologies, including encryption and multifactor authentication (or risk-based authentication), among others;
- Conduct regular security assessments, including penetration testing, and vulnerability and risk assessments;
- Ensure that senior management (or the board chair) files an annual certification confirming compliance (much like reporting on internal controls under Sarbanes-Oxley);
- Provide regular cybersecurity awareness training for all personnel;
- Create a written incident-response plan;
- Maintain a system that includes audit trails for reconstructing financial transactions and confirming obligations, and retain these records for not fewer than five years; and
- Report to a governing authority (such as the NYDFS) on any cybersecurity event "that has a reasonable likelihood of materially harming any material part" of the organization's normal operations.[iii]

The Compliance Challenge

Compliance with Part 500 will require resources – personnel and money – that may need to be diverted from core business activities, plus expertise that not all organizations possess.

Overall there is a lack of cybersecurity talent, experience, and expertise in the market. For example, in 2015 over 200,000 cybersecurity positions went unfilled in the United States, according to a Stanford University analysis of data from the U.S. Bureau of Labor Statistics. Some reports expect the global security labor shortfall to reach 1.5 million by 2020. This shortage means that companies – not just insurance firms – have to pay top dollar to recruit and retain this workforce.

CISOs with the requisite experience and knowledge of the data security world are scarce and, not surprisingly, expensive to retain. Under Part 500, firms are required to maintain a CISO, and as demand for their services increases, so have their salaries, with total CISO compensation at large firms reportedly approaching or topping $1 million.

Beyond the talent crunch, the continuous monitoring required by Part 500 is not specifically defined and therefore will require skilled experts to implement technically. However, this implementation is not just a technical issue – it must be folded into a holistic cybersecurity risk management decision that also considers the requirements of business. This demands talent, experience, judgment, and appropriate policies and procedures.

Finally, the type of reporting mandated by Part 500, and the responsibility it places on the board and senior management, necessitates a focus that makes cybersecurity and cybersecurity awareness a more organic part of the company's culture. And that kind of organizational change is always hard, especially in today's difficult market environment in which insurers are under intense pressure to lower costs while modernizing their information technology (IT) systems to create new products and services to boost top-line revenue. It will require a level of training, awareness, and involvement across the entire company.

The underlying financial investment that will be required for achieving compliance will certainly not be small. While larger firms should be able to manage the costs, the costs could be overwhelming to small-to-midsize insurance firms. However, no matter the difficulties, if financial services organizations and insurers wish to do business in New York, they must work to overcome these challenges.

Toward a Holistic Security Program

A compliant, effective cybersecurity program should be an integral part of an organization's enterprise risk-management strategy. Minimizing cyber risk means an organization should:

- Identify critical data assets and protect them appropriately;
- Conduct a thorough organizational review to find and remediate gaps between written policies and procedures and business operations and transactions;
- Examine the processes that will produce reporting in case of an incident;
- Create an actionable, written data-breach response plan that includes both internal and external communication strategies;

- Implement processes for continually updating security systems, including patch management. (The May 2017 WannaCry/WannaCrypt ransomware attack used a vulnerability that took advantage of unpatched and outdated systems. Britain's National Health Service was one such victim, and this ransomware attack brought many of their systems' operations to a halt, potentially placing lives at risk.)
- Conduct cyber awareness training throughout the enterprise at least once a year.

These and other actions should be conceived as part of a holistic security program, founded upon a comprehensive understanding of cybersecurity risk, with written policies and procedures broadly communicated to all parts of the operation. These policies and procedures should always be accessible and available to regulators to demonstrate the organization's adherence to its own written policies. There must also be a confirmatory audit trail designed to allow companies and regulators to reconstruct material financial transactions, as well as a record of cybersecurity events and the company's processes of detection and response. Boards of directors should prioritize making risk determinations and ensuring compliance with the various requirements of Part 500.

As insurance companies modernize their IT systems, cybersecurity must be baked into their plans, not treated as an afterthought. That means properly trained security experts must be a part of any modernization effort, sitting side-by-side with developers, planners, and line-of-business leaders.

If in-house expertise is lacking, firms may consider outsourcing various elements of cybersecurity preparedness and monitoring to experienced and well-vetted third parties. However, organizations must understand that, although Part 500 permits the outsourcing of penetration testing, vulnerability assessment, and other cybersecurity risk-mitigation activities, even including engaging a third party to fill the CISO role, the covered entity ultimately remains responsible for security and for compliance with Part 500.

Therefore, while outsourcing arrangements can be enormously beneficial in helping firms fill gaps in personnel, experience, and expertise, they should be entered after a rigorous due-diligence process and with a well-considered plan for governing and monitoring this critical relationship with full transparency and a robust reporting process.

The Compliance Opportunity

Compliance does not in and of itself equal security, and if complying with Part 500 is approached as a check-the-box exercise, it won't enhance security. A company that can see the compliance process as an opportunity to not only become a more secure organization, but also a more efficient one, is primed to reap the full benefits of becoming both more secure and more operationally efficient.

For example, some organizations have invested in deploying security applications for two-factor authentication on mobile work phones. This allows their people to access the information they need to conduct business on a more secure connection, even in an insecure environment such as an airport. In this case, security is enhanced while also increasing workforce efficiency and the organization's profitability.

The process of thoroughly examining existing procedures and policies and developing more secure ones can enable a firm to learn about and incorporate up-to-date best practices and operational controls, not only in security but also in organizational governance. This is the opportunity that compliance affords, and all firms may benefit from it in many ways if they embrace the cultural transformations it entails.

New York State Department of Financial Services, 23 NYCRR 500, "Cybersecurity Requirements for Financial Services Companies," Introduction.

Ibid. Non-public information is defined in Section 555.01, Part g, 1 – 3.

Ibid., Section 500.17, Part a., 1 – 2.

*This article first appeared in *Insurance Journal* on October 10, 2017

Anthony J. Ferrante
Senior Managing Director,
Leader of the Cybersecurity practice
+1 202 312 9165
Anthony.Ferrante@fticonsulting.com

Jimm Wrynn
Senior Managing Director
Global Insurance Services
+1 212 841 9366
Jim.Wrynn@fticonsulting.com