July 26, 2019

Poor Richard Brings His Cybersecurity Kill Chain to New York's SHIELD Act

by Jon Neiditz

Poor Richard does get his hoped-for trip to New York today, but not, as many others hoped a few months ago, to examine a new comprehensive privacy law that outdoes the CCPA with the first enactment of the concept of data fiduciary responsibility for businesses and other innovations. No, instead of unsheathing that sword, the New York legislature chose the SHIELD Act, which updates its general breach law to incorporate the innovations of many other states, SHIELD also creates a general affirmative duty of reasonable security beyond the financial, health and other regulated sectors, a requirement more prescriptive than many but still risk-based (and less prescriptive than Massachusetts' 201 CMR 17.00) and in the great tradition of such reasonable security requirements since Section 1798.81.5 of the California Civil Code was first enacted in 2004.

Between SHIELD and the tougher requirements on financial institutions of 23 NYCRR 500, New York firmly establishes itself as one of the high-bar states for breach notification and general security, yet it does so in SHIELD through a law that does not require any sea changes in security programs that comply with other laws except in the one case noted below. In those senses, Poor Richard approves of SHIELD as a well-drafted law that brings New York to the forefront but does not establish an untested, new bleeding edge, while satisfying both the tech industry and Consumer Reports.

SHIELD's Most Important Provisions

1. New, demanding "harm" standard – The one area in which SHIELD significantly departs from precedent is the new harm standard, which draws on innovations such as Florida's, but goes beyond them in several ways:

> "Notice to affected persons under this section is not required if the exposure of private information was an inadvertent disclosure by persons authorized to access private information, and the person or business reasonably determines such exposure will not likely result in misuse of such information, or financial harm to the affected persons or emotional harm in the case of unknown disclosure of online credentials as found in subparagraph (ii) of paragraph (b) of subdivision one of this section. Such a determination must be documented in writing and maintained for at least five years. If the incident affects over five hundred residents of New York, the person or business shall provide the written determination to the state attorney general within ten days after the determination."

This provision is probably the reason that savvy consumer advocates like Justin Brookman say SHIELD is good law, with its (a) allowing a "risk-of-harm" exception only in the context of inadvertent disclosures by authorized personnel, (b) specifically establishing “emotional harm” as a standard, and (c) requiring that determinations of no harm in large breaches go to the AG in 10 days. Poor Richard is not quite as happy about this provision for our clients, but knows how we will deal with it and what we will begin to share with the New York AG that the Legislature may have missed. We will even tell you about it toward the end of this post.

2. Expansion of notice-triggering information:

a. Like a minority of other states following the Yahoo and LinkedIn breaches, New York now includes credentials (password or security question and answer) that would permit access to such online (non-financial) accounts.

b. New York joins the growing number of states that include biometric information.

c. New York also joins a minority of other states in treating account number or payment card number as notice-triggering if they could be used to access a financial account without an access code or other additional information.

3. An “access or acquisition” state: New York joins the minority of states that defines breach in terms of both unauthorized access and unauthorized acquisition of notice-triggering information.

4. Tell the AG about HIPAA breaches. Many breaches of PHI are not breaches under state law, but in New York you will need to tell the AG about them.

5. Reasonable, risk-based security standards: The standards, while comprehensive, are all reasonable and based on risk assessments. They include a scalability provision for small businesses, but even medium-sized businesses can use their risk-basis as grounds for scalability. The comprehensiveness of the standards, however will no doubt push both small and medium-sized businesses more quickly into the more secure cloud offerings.

Kill Chains for the New Harm Standard

Like anyone worth their salt in incident response, Poor Richard has been using the ideas generated by the concept of the “kill chain” to prevent harm precisely in attacks by malicious outsiders and insiders, i.e., exactly those incidents that may not even be eligible for a determination of “no harm” under SHIELD, which in effect prevents such a determination if there is malice such that the disclosure is not entirely “inadvertent.” As Clarke and Knake recently observed, the kill chain turns the advantage from the attacker to the defender because the many steps the attacker must take each become a focus for disruption. Disrupting a necessary step in the chain prevents harm. Productive conversations with the New York Attorney General’s Office to follow.

What it Means: Stasis, Philetic Gradualism or Punctuated Equilibria?

SHIELD is a good, strong law that puts New York on the forefront of cybersecurity regarding personal information across all industry segments – as it already was in financial services – without forcing material

changes in effective security programs. Its comprehensive yet risk-based security standards are particularly laudable. Its passage rather than passage of the comprehensive data protection bill that had been introduced in New York tells us a lot about what's really going on in this supposed year of GDPR- and CCPA-inspired legislation across the U.S. It is not just stasis either; in addition to the security standards that reflect decades of learning, Poor Richard's kill chain points out one way in which its one step beyond both the laws of other states and its own law will lead to legal and technical innovation in incident response.

In choosing relatively conservative security/privacy law rather than bleeding edge law, New York provides more evidence, as Poor Richard has been saying in his other posts, that 2019 expectations for comprehensive privacy laws sweeping the states and at the federal level has been principally wishful thinking and fear-mongering. Poor Richard has long hoped that the combination and breach notification invented by California in 2002 through 2004 could evolve to help foster the cyber-awareness and preparedness that we need, and SHIELD – with its security standards and incorporation of important innovations from other states – is the best product of that gradual evolution. The question now is whether (1) we are stuck with that philetic gradualism because, even though it doesn't address most of the big current and future privacy issues that the public and even politicians now talk about, politicians can muddy the waters by saying that they have acted to protect privacy, or whether (2) the series of fortunate and/or unfortunate events that resulted in the CCPA will lead to punctuated equilibria notwithstanding the global failure to create effective privacy regulation in this period of tribal partisanship.

To explore that last issue, we may need to include one of our other colleagues we have been wanting you to meet rather than Poor Richard, given that Poor Richard's vision is not only enhanced but limited by his helpful pragmatism.