From the Sponsor EXECUTIVE FORUM **CYBER SECURITY**

The Big Data Breach - For the Rest of Us

By now, reporting on large-scale data breaches has become ubiquitous. Be it Target, Anthem or the N.S.A, we have become accustomed to the idea that the bigger the aggregation of data, the greater the risk. But while, or perhaps because, big data has been hardening its perimeter, a sea change has occurred, surprising many in the business of securing our data. The threat to data, regardless of type or size, has been democratized. Entities and systems of all levels of complexity are now at risk, as the business of the data breach booms.

The first indication of this sea change is the rise in ransomware. Whether in the form of "locking" malware, such as Petya, which prevents access to the affected system, or a more traditional "crypto" attack, which can encrypt user files stored on the system, the genius in ransomware is its simplicity. The value of the data at issue to the attacker is irrelevant. It is the value to the victim of having access to its data that sets the market price for the ransom. And the majority of ransomware attacks tend to be automated, issuing from servers running around the clock, or even from "ransomware as a service," now available to would-be cyber extortionists lacking in technical expertise. Ransomware has effectively no overhead, only the potential for millions of dollars in returns.

The rise in ransomware has caught some of the most sophisticated players in the information security space unawares. At least one of the major global players in the IT forensics and information security space recently announced extensive layoffs because of the rise of ransomware. The entity had expected to see an increase in directed threats, which can require more detailed forensic analysis than a simple ransomware attack. Ransomware is often the result of a single click upon an infected e-mail or attachment, not a complex, individualized attack on a system.

F. Paul Greene
Partner, Chair Privacy and Data Security Practice,
Harter Secrest & Emery LLP

HSE
Harter Secrest & Emery LLP
ATTORNEYS AND COUNSELORS

The second indication is the rise in regulation. Currently, 47 states (as well as the District of Columbia and Puerto Rico), have data breach notification laws on their books, most of which are enforceable by the relevant state attorneys general. These laws generally require notice to affected individuals as well as, quite often, state authorities and law enforcement. As of the time of this article, no fewer than ten different states have pending legislation proposing changes to their notification laws. As one would expect, via these changes, states are increasing the controls they put on data security and breach notification, not decreasing them. And a number of states remain agnostic as to where the breach occurs. As long as the breach involves data concerning a resident of the state, regardless of where the breach occurs, these states demand compliance with their notification and, at times, substantive security requirements. Not only does this affect nationwide retailers, it can affect any entity with customers or employees, even retirees, resident in other states.

> We have become accustomed to the idea that the bigger the aggregation of data, the greater the risk.

Beyond the state level, the federal authorities have increased enforcement efforts, but no uniform standard applies. The Federal Trade Commission, for example, regulates data security under its mandate to combat "unfair" and "deceptive" business practices. Yet no regulations underlie the FTC's authority in this regard. Rather, the FTC points to at least seven different sources for guidance on what it considers to be "reasonable" in relation to data security: "[FTC] speeches, business education, Congressional testimony, articles, blog entries, . . . as well as other FTC settlements in the data security area." Needless to say, a standard that one must piece together from a myriad of possibly conflicting sources is no standard at all.

Third is monetary risk. The costs of a data breach are increasing. According to one report, for a modest-sized breach of 10,000 records, direct breach-related costs can amount to $4.9 million or more. Included in that number are, for example, forensic costs and fines, both of which are increasing. The New York State Attorney General recently announced one of its largest fines in the data breach space: $100,000 to an on-line retailer for security and breach notification failures. On the federal level, the FTC can issue fines as well, and its standard form of consent order includes 20 years of data security monitoring and reporting to the FTC, binding on a company's successors and assigns.

Taken together, these three developments show that the risk of a data breach is no longer reserved to large aggregators of data. The risk has spread to small and medium businesses, to large non-retail businesses, to entities of all size and description that value their data, i.e., to the rest of us.