THE COMING OF THE CYBER MONITOR

Regulators, like prosecutors, are increasingly turning to independent monitors as a means of moving non-compliant entities into compliance. It appears certain that the appointment of independent monitors to enforce compliance with cybersecurity regulations will become common. Several financial industry regulators are moving to establish cybersecurity standards with which financial institutions will have to comply just as they do with money laundering and other regulations.

This past November, the New York State Department of Financial Services issued a memorandum to numerous other federal and state financial services industry regulatory agencies concerning cybersecurity in that industry. The memorandum called for all the agencies to work together to create a comprehensive regulatory scheme to mandate certain cybersecurity practices and procedures. The document identified several concerns:

- Cybersecurity challenges will continue to be driven by technological changes and the increasing sophistication of attacks.
- Third party vendors will remain important attack vectors.
- The risk is global.

The Department stated that the expected regulations "would require covered entities to maintain a cyber security program designed to perform core cyber security functions and would set specific requirements" for written policies and procedures addressing not only its own operations but those of third party vendors, as well, and for the use of multi-factor authentication for several types of transactions, including customer access. This initiative is in full accord with efforts of the Securities and Exchange Commission and the Commodities Futures Trading Commission to promote and require adequate cybersecurity practices within their regulated entities.

Regardless of what form the regulations ultimately take, rest assured they are coming, and perhaps not only in the financial industry. The next step, of course, is enforcement. Future network intrusions will not only require incident response and data breach notification compliance, but formal explanations to a regulator as well. As the stakes get higher, the need for adequate security compliance grows stronger.

Financial institutions and other regulated entities are commonly subject to the imposition of a monitor by state and federal regulators to address a wide range of misconduct. Having inadequate controls to detect and prevent money laundering is a prime example. With so much at risk from intrusions into financial industry systems, and indeed all data-intensive networks such as the health care industry, the imposition of an independent monitor to move the entity into compliance can only be accepted as the coming norm.

Thus, it may become most prudent to add a cyber monitor to your incident response team. We all recognize the need for counsel, the forensic investigators, internal IT, and perhaps a public relations firm, but the cyber monitor just might become an essential component as well. As the incident investigation unfolds, the forensic investigator and internal IT work to find out what happened and counsel evaluates the resulting legal consequences and obligations. But in anticipation of the looming response of the regulators, the cyber monitor begins at as early a stage as possible to identify and repair lapses in compliance. Using the recently issued Yates Memorandum by the U.S. Department of Justice as an example, the steps an entity takes on its own to identify and remedy misconduct and regulatory violations can go a long way to minimizing the sanctions imposed by a regulator.

The difference between a computer security company and a cyber monitor is important. The former is a technical expert in cyber forensics, networks and penetration testing. The monitor possesses a very different set of expertise, upon which we will comment in our next installment.