February 23, 2018

Federal Enforcement Agencies Take Action on Cybersecurity

Jack Theis and Kelly M. Warner

Cybersecurity risks pose substantial challenges to any company functioning in today's data-driven marketplace. In addition to threats from internal and outside forces, risks associated with protecting personal and financial information, and the possibility of protracted civil litigation, corporations face increasing pressure from regulators to ensure the security of their systems. This week, the federal government doubled down in this arena: the Department of Justice established a task force to combat cybersecurity threats, and the Securities and Exchange Commission issued guidance on the appropriate disclosures of cyber risks and incidents.

DOJ Establishes Task Force on Cybersecurity Threats

On Tuesday, in a memorandum issued by the Attorney General, the Department of Justice announced the establishment of a task force combatting cybersecurity threats. While media reports have highlighted the Cyber-Digital Task Force's focus on interference with elections, the task force is also directed to address risks of corporate theft and the security of consumer information. The task force will analyze how DOJ currently combats global cyber threats and will identify areas where law enforcement can more effectively protect the government, private citizens, and corporate entities from the malicious use of technology. Establishing a task force often signals increased enforcement or regulatory engagement, and Tuesday's announcement echoes previous DOJ efforts to combat financial and intellectual property crimes.

The Attorney General identified several cybersecurity threats that impact consumers and businesses, including the "theft of corporate, governmental, or private information on a mass scale" and the "mass exploitation of computers, along with the weaponizing of everyday consumer devices . . . to launch attacks on American citizens and businesses." These threats are well known, and well respected by in-house counsel and corporate boards. From

the data breaches at major corporations to the increased frequency of DDoS attacks, companies operating in the global marketplace face the daily risk of attack from third parties. The task force will identify ways in which law enforcement can assist corporations—or ensure corporations are on top of—risks of these large-scale attacks.

The Cyber-Digital Task Force will be chaired by a senior DOJ official appointed by the Deputy Attorney General and will consist of representatives of various Department components, including the FBI, the Criminal Division, the National Security Division, and the United States Attorney's Office. DOJ may also invite membership from other federal agencies; the Department of Homeland Security, the Federal Communications Commission, and the Federal Trade Commission are likely candidates.

The Attorney General requested an initial report from the task force by June 30, 2018.

SEC Guidance on the Disclosures of Cybersecurity Risks and Disclosures

On Wednesday, the Securities and Exchange Commission announced the adoption of long-awaited interpretive guidance to assist public companies in preparing disclosures about cybersecurity risks and disclosures. In a press release accompanying the guidance, SEC Chairman Jay Clayton stated that the guidance "will promote clearer and more robust disclosure by companies about cybersecurity risks and incidents, resulting in more complete information being available to investors."

The new guidance reinforced existing guidance from 2011 on the appropriate disclosure of cybersecurity incidents and expanded on two additional topics, both of which demand that corporations address and track cyber risks and incidents. First, the SEC stressed the importance of maintaining comprehensive procedures related to the disclosure of cybersecurity incidents. Under Exchange Act rules, companies must maintain controls and procedures governing how and when to make appropriate disclosures. The SEC recommended that companies undergo a careful review of those controls and procedures to make sure that, in the specific context of a cybersecurity incident, the relevant information gets to the right personnel for disclosure decisions. It should now be abundantly clear that SEC disclosures are among the myriad issues in-house counsel is to consider following a cyber incident.

Second, the SEC emphasized that making selective disclosures of material nonpublic information about cybersecurity risks or incidents can invoke insider trading law. The SEC specifically suggested that companies consider implementing restrictions on insider trading during the investigation of an incident and prior to a public disclosure.

Riley Safer Holmes & Cancila LLP's cybersecurity team will provide additional updates on enforcement priorities, the regulatory environment, and any additional agency guidance related to cybersecurity risks and incidents.

For further information, **please contact:**

Kelly M. Warner
1.312.471.8740
kwarner@rshc-law.com
Chicago

Jack Theis
1.312.471.8761
jtheis@rshc-law.com
Chicago

Ryan P. Poscablo
1.212.660.1030
rposcablo@rshc-law.com
New York

About Riley Safer Holmes & Cancila LLP:

Riley Safer Holmes & Cancila LLP (RSHC) is a diverse, service-oriented, and technologically sophisticated firm that is committed to providing legal and client service at the highest levels. We are determined to redefine the traditional relationship between law firms and companies by making sure that our needs and goals are always aligned with those of our clients.

RSHC is a national law firm of trial lawyers and transactional attorneys with offices in Chicago, San Francisco, New York, and Ann Arbor. The partnership team features leaders in many practice areas, including antitrust, business transactions, class actions, white collar, product liability, intellectual property, and general litigation. Diversity begins with the names on the door and extends through the partnership and associates ranks. RSHC is home to more than 70 lawyers, seven of whom are former Assistant United States District Attorneys.