Independent, Disinterested Cyber Advice Can Help Your Bottom Line

Since cybercrime is on the increase,[1] business executives and board of directors' members sometimes feel pressure to make hasty decisions involving cybersecurity matters without sufficient deliberation of information. Often corporations make costly expenditures that exceed the amount of money on cybersecurity that has to be spent to achieve the relevant objectives. Due to the absence of corporate experience in the cybersecurity area, the risk of undue reliance on actors in the cybersecurity industry is not uncommon.

As a result, business organizations can benefit from independent, disinterested, specialized legal assistance. I can provide a range of services that might reduce your future expenses and in some cases even generate revenue, by:

- serving as an expert witness or source of information on cybersecurity regulatory matters;
- organizing and conducting internal investigations;
- evaluating the reasonableness of outside counsel fees;
- reviewing the suitability of a cybersecurity insurance policy or comparing a number of cybersecurity policies to facilitate the decision-making process within the corporation; and
- assessing suitability of cybersecurity tools sold by suppliers.

When required, I rely on Thomas Welch, a lawyer specializing in cyber-related matters in the health sector (legal, litigation and regulatory issues primarily for conducting internal investigations)[2] and Rick Dregar (cybersecurity technology issues).[3]

The government bodies' responsibilities and the rules they are to enforce are constantly changing, as are the actual regulations and other norm-establishing documents. Business organizations have difficulty operating in such environments. As a consequence, they have a strong need for timely and accurate information concerning changes in cybersecurity regulations or actual enforcement practices, for example, when the Framework for Improving Critical Infrastructure Cybersecurity, released by the National Institute of Standards and Technology was issued, "it was intended . . . as a guide to the private sector to develop best practices."[4]

---

[1] *See http://www.bjs.gov/index.cfm?ty=tp&tid=41*, http://www.justice.gov/usao/priority-areas/cyber-crime https://www.dhs.gov/topic/combating-cyber-crime, and http://www.wired.com/insights/2014/10/cybercrime-growth-business/.

[2] See http://www.ThomasWelchLaw.com.

[3] https://www.wavegard.com/why-wavegard/rick/'

[4] SEC Commissioner Luis A. Aguilar, Address at "Cyber Risks and the Boardroom" Conference. June 10, 2014, available at https://www.sec.gov/News/Speech/Detail/Speech/1370542057946, *Last Visited February 27, 2016)*

Nonetheless, the SEC viewed the non-compliance with the Framework to be a violation of the securities laws. If a business were basing its cybersecurity procedures on the basis of the written law, it may be regarded be subjected to fines. This is a good illustration of why businesses cannot rely solely on the written law in the area of cybersecurity.

There is a tendency of some to view corporate cybersecurity policies within a risk management[5] framework, where Risk = Threat * Probability. In this context, the goal is to either reduce the size of the "threat" or to reduce the probability of an "attack". Corporations face a range of threats making the calculation of risk impossible. Basically, there is a lack of data for planning purposes.

To accurately assess the risk to the corporation, such a formula would have to account for numerous unknown variables: (i) the identity and characteristics of the attacker, (ii) the tools available to the attacker, and (iii) the goal(s) or objective(s), resources, strategy, tactics, and determination of the attacker. Hence, determining "risk" with any degree of confidence would appear to be an impossible task.

Nevertheless, certain threats can be anticipated. For example, the legal consequences for failing to comply with government-established standards and the financial costs associated with specific actions. Businesses can incur expenses as a result of changes in laws, regulations, rules, practices and procedures, or as a result of important judicial decisions.

A large share of cyberattacks are carried out by insiders.[6] It is difficult for an organization to investigate its own personnel without it having potential negative consequences. Similarly, it is not advisable to include in an internal investigation team someone who may have been involved with the wrongful act(s) or know the actual wrongdoer or negligent individual. As a result it is often useful to use an outsider to conduct the investigation. Sometimes it is advisable to use a small team to conduct an initial investigation, rather than arrange for a level of effort that exceeds the actual need. Of course, this all varies on a case-by-case basis.

* * * * *

---

[5] *See "* The Communications Security, Reliability and Interoperability Council, Cybersecurity Risk Management and Best Practices Working Group: Final Report," March 2015, available at https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf FINRA, "Report on Cybersecurity Practices," February 2016, available at https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf and Kristin N. Johnson, "Cyber Risks: Emerging Risk Management Concerns for Financial Institutions," 50 Ga. L. Rev. 131 (2015) available at http://heinonline.org/HOL/LandingPage?handle=hein.journals/geolr50&div=9&id=&page=.

[6] *See* http://www.csoonline.com/article/2908475/security-awareness/surveys-employees-at-fault-in-majority-of-breaches.html, www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/managing-insider-threats.pdf, http://www.securityinfowatch.com/article/10510466/the-insider-threat http://www.securitymagazine.com/articles/85081-how-to-reduce-the-insider-cyber-threat.