Leadership and Cybersecurity

By Alan S. Wernick, Esq.

Will Rogers is quoted as saying: "People's minds are changed through observation and not through argument."[1] Business leaders do make a difference when it comes to data breaches and cybersecurity threats – which are almost a daily news item. Losses due to a data breach are expensive, particularly in a reactive (versus proactive) mode, and may include loss of trade secrets and other intellectual property assets; personal identifiable information ("PII") – credit card, financial, and medical data of customers, employees, and/or suppliers; loss of business goodwill; and loss of other valuable business assets. Empirical data, statutes/regulations, and developing case law underscore the compelling need for business leaders to proactively understand, identify, and manage cybersecurity legal and technology risks.

There have been several recent studies indicating the power of C-Suite's[2] leadership impact on a business' cybersecurity risks. A May 2016 study by the Ponemon Institute[3] titled "Tone at the Top and Third Party Risk" provides several interesting insights into business leadership and cybersecurity including:

- "Most C-level executives are not engaged in their organization's third party risk management process. Only 37 percent of respondents agree that the C-level executives in their organization believe they are ultimately accountable for the effectiveness of third party risk management. As a possible consequence of this lack of engagement, 50 percent of respondents do not believe the risk management process is aligned with business goals, which are most likely determined by senior management."
- "The CEO is expected to set a positive tone. Forty-one percent of respondents say it should be the CEO who sets the tone at the top, followed by 19 percent of respondent who say it is the compliance officer. Only 6 percent of respondents say the C-suite is most responsible for setting a positive tone at the top for the entire organization."
- "The consequences of not managing third party risk can be costly. In the past 12 months, organizations represented in this research spent an average of approximately $10 million to respond to a security incident as a result of negligent or malicious third parties."
- "Most C-level executives are not engaged in their organization's third party risk management process. Only 37 percent of respondents agree that the C-level executives in their organization

[1] Anyone who is a parent may have discovered this to be true….
[2] E.g., "CEO" – Chief Executive Officer; "CFO" – Chief Financial Officer; "COO" – Chief Operating Officer; "CIO" – Chief Information Officer.
[3] The Ponemon Institute (www.ponemon.org) conducts independent research on privacy, data protection and information security policy. Alan is one of several Ponemon Institute Fellows.

believe they are ultimately accountable for the effectiveness of third party risk management. As a possible consequence of this lack of engagement, 50 percent of respondents do not believe the risk management process is aligned with business goals, which are most likely determined by senior management."

- "Boards of directors are not actively engaged in risk management activities. Similar to the perceived lack of accountability on the part of C-suite executives, only 40 percent of respondents say their boards of directors are significantly involved (17 percent) or have at least some involvement in overseeing risk management activities (23 percent)."

So what, if anything, can the C-Suite and the Board of Directors do about cybersecurity threats to their business? "It depends" is probably the best answer. Members of the Board of Directors may not be required to have a detailed understanding of the applicable technologies, and may be able to rely, in part, on outside experts in evaluating and managing cybersecurity risks. When an active cyber threat is discovered (e.g., a data breach), their actions pre and post breach may be subject to review in any resulting litigation under the applicable law of the business judgment rule to determine if they followed the appropriate standards of care, loyalty, and good faith. Most likely, that analysis will depend on whether the actions (or inactions) taken by the C-Suite and the Board of Directors were reasonable and reflected good common sense in comparison to their peers in their industry.

There are a number of variables in play for cybersecurity risks for each business, including the industry, the applicable industry regulations and standards, the available skill set (e.g., does the CEO or CFO also have to function as the CIO and/or CPO for the business, or does the business have individuals with the appropriate experience in those roles; do the CEO and CFO have a technology background and/or experience), and the available resources for proactive versus reactive costs related to cybersecurity incidences, among other factors. The following, while by no means an exhaustive list, provides ten (10) initial items for consideration:

1. What assets are at risk? Examples include trade secrets and other intellectual property assets; personal identifiable information ("PII") – credit card, financial, and medical data of customers, employees, and/or suppliers; business goodwill; and other valuable intangible business assets.
2. Where are the assets stored? For example, are they stored in "the cloud," on a computer server with no connection to the Internet, in the United States or elsewhere?
3. Who has access to the assets? For example, what is the authorization/access protocols and hierarchy for each asset and how often is it verified and updated (e.g., does an employee departure automatically trigger an update to the authorization)?
4. What assets are encrypted and are they encrypted at all times (e.g., including in transit within and outside the business)?
5. When does the business do penetration testing to test for vulnerabilities?
6. What type of insurance coverage for cybersecurity risks of the business is in place and is it adequate for the cybersecurity risks confronting the business?

7. What types of physical (e.g., the secure and locked door) security and technology (e.g., firewalls, software monitoring tools, etc.) security are used for all of the assets?
8. How familiar are the C-Suite and the members of the board of directors (and members of committees of the BOD) with cybersecurity risks and compliance? What is their level of understanding of the different types of cybersecurity risks and the types of harm they may cause a business? Are they familiar with their industry standards concerning cybersecurity risks (for example, the NIST Cybersecurity Framework)? How will their actions (or inactions) be viewed in light of the applicable law of the business judgment rule if the board's failure to manage cybersecurity risks rises to the level of a breach of fiduciary duty?
9. What employee training programs, if any, are conducted by the business? And, what are the frequency and effectiveness of the training? Recent studies have shown that insider threats continue to pose increasingly significant privacy and cybersecurity problems for businesses. Sometimes that threat is from the intentional actions of a disgruntled employee, and sometimes the threat arises because of the uninformed employee (e.g., "I thought that e-mail asking me to transfer a million dollars to customer X's bank account was really from the CFO….").
10. When, if ever, did the business have a legal audit performed (e.g., a privacy audit or an intellectual property audit)? How frequent are these legal audits and are they being conducted by knowledgeable legal counsel?

While the above is not an exhaustive list, how comfortable are you with knowing the answers to these questions for your business? As the Chinese military general Sun Tzu said in "The Art of War:" "The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable."

The bottom line is cybersecurity risk correlates to whether or not the C-Suite and Board of Directors take the time to understand privacy and cybersecurity risks and embrace, educate, and manage as leaders in cybersecurity risk mitigation strategies appropriate to their business.

For comments about this article or to be added to the *ITIP Alert™* subscriber's list, please contact ALAN WERNICK (E-MAIL: ALAN@WERNICK.COM; PHONE: 847.786.1005 OR 614.463.1400).