NYSE Governance Services

A 2015 SURVEY REPORT

Cybersecurity and Corporate Liability: The Board's View

VERACODE

The continuous emergence of digital innovation, the ongoing revelations of high-profile data breaches, an increasing level of marketplace activism, and companies' ever-growing reliance on the digital space have all contributed significantly to bringing cybersecurity matters to the forefront of board and senior management discussions.

If the recommended methods to protect a business's most valuable assets—its brand integrity, intellectual property, and sensitive customer information—remain difficult to grasp and implement by many, there is much to be said about the critical issue of ensuing corporate liability in the event of a data breach should those methods fail.

The 2015 Volkswagen emissions control software scandal clearly demonstrates the impact corporate liability issues can have on reputational integrity and brand value. Consider that today, according to Forrester Research, "at least 88% of the S&P's market value consists of goodwill and intangible assets, such as reputation, brand, innovation, processes, know-how, and customer experience. Go back to 1975, and only 17% of market value was goodwill and intangible assets[1]." Security is the second leading risk to a company's brand, behind ethical issues and ahead of risks related to safety, health, and the environment[2]. This only increases the pressure on boards and management teams to be especially wary of any corporate behavior that can lead to liability issues.

Determination of responsibility in the case of a cyber breach is a key question; yet, several other questions are critical to framing discussions around cyber liability. Among them:

• Who should be tasked with monitoring businesses in their cyber defense efforts? Should it be in the hands of regulators, or will civil lawsuits by affected customers and investors be sufficient to curb negligent behavior?

• When should a company be considered negligent in its processes—or lack thereof—of securing sensitive information, and what constitutes "reasonable efforts" to address vulnerabilities in networks and software, such as web applications, databases, libraries, and frameworks?

• Is cyber insurance sufficient on its own to preserve value at the corporate level?

While these questions most often sit at the IT level, it is interesting to note that the extent of the brand damage caused by breaches is often linked to boards' level of preparedness. It is therefore a board's fiduciary duty to ask the right questions to ensure due care has been followed.

As a result, NYSE Governance Services, in partnership with Veracode, surveyed 276 directors and officers across publically traded companies to draw parallels between businesses's cyber risk management practices and their efforts to address cybersecurity liability matters. Our goal was to provide further benchmarking practices to serve the interests of public companies' boards of directors and their shareholders.

Nine out of 10 directors and officers believe regulators should hold businesses liable for breaches if they don't make reasonable efforts to secure customer data.

The great majority (89%) of surveyed directors and officers believe that a company that does not make reasonable efforts to secure its data should be held liable by regulators (Figure 1).

Similarly, 90% agree that third-party software providers should be held liable when vulnerabilities are found in their packaged software (Figure 2). And coinciding with the U.S. Securities and Exchange Commission's intensified focus on third-party risk management, two-thirds (65%) of respondents say they have already begun or are planning to insert liability clauses into contracts with their third-party providers.

This is particularly relevant because according to Veracode's 2015 State of Software Security Report, nearly three out of four enterprise applications produced by third-party software vendors contain vulnerabilities listed in the OWASP Top 10, an industry-standard ranking of critical web application vulnerabilities that should be remedied as a matter of course.

One question that remains is what constitutes failing to take "reasonable efforts." In other words, what constitutes negligence? For instance:

• The JPMorgan Chase Corporate Challenge website and British telecom provider TalkTalk were breached through what appears to be a common application vulnerability called SQL injection (pronounced "sequel injection")[3,4].

SQL injection has been listed on the industry standard OWASP Top 10 for more than a decade. Should TalkTalk or the third-party contractor who built and managed JPMorgan's charity site be liable for not finding such a common vulnerability?

• The Verizon 2015 Data Breach Investigations Report (DBIR) shows that 99.9% of the Heartbleed-like software vulnerabilities exploited in 2014 were publicly announced more than a year before they were exploited, with some vulnerabilities going back to 1999[5]. Is it "reasonable" not to patch a known vulnerability, and should businesses be held liable for failing to do so?

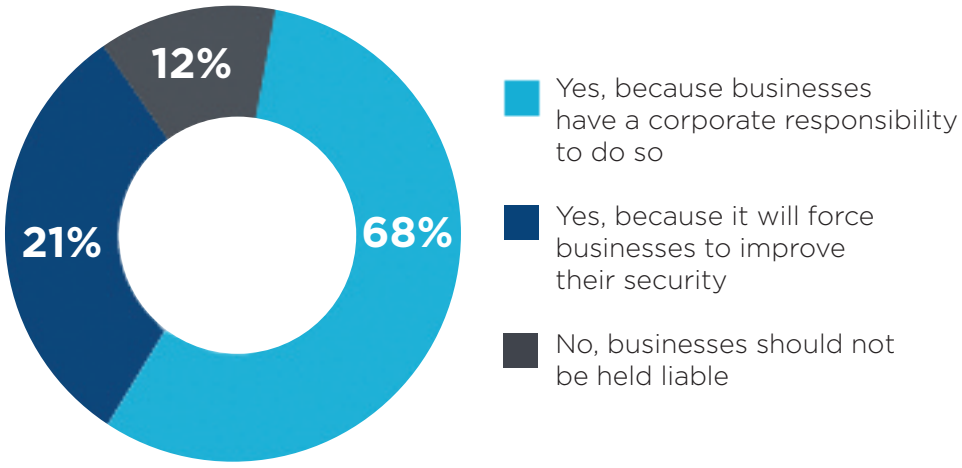
• Studies have shown that "companies that have a dedicated CISO (Chief Information Security Officer) detected more security incidents and reported lower average financial losses per incident[6]." Can we assume that a company that does not have a CISO is not making a reasonable effort to secure data?

Considering the growing threat of legal action over cyberattacks, boards have a fiduciary duty toward shareholders to ensure management has instituted appropriate controls. Increasingly, investors are beginning to understand the impact of such incidents and are seeking definite answers on how the businesses they invest in mitigate cybersecurity risk.

The Wyndham Worldwide lawsuit has influenced executive discussions on cybersecurity liability.

Almost half of directors and officers who were familiar with the Wyndham Worldwide lawsuit at the time of our survey say the case has influenced their executive discussions on cybersecurity liability.

FIGURE 1
Should regulators hold businesses liable for breaches if they don't make reasonable efforts to secure customer data?



For those unfamiliar with the case, the FTC alleged that the global hotel chain had violated Section 5 of the FTC Act by failing to employ reasonable data security measures, including the use of vulnerable out-of-date software[7], which in turn led to a breach involving sensitive customer information. According to the complaint, these failures resulted in more than $10 million of fraudulent charges on consumers' credit and debit cards, as well as the transfer of hundreds of thousands of consumers' account information to a website registered in Russia. Wyndham Worldwide argued these claims by challenging the FTC's authority to regulate companies' data security standards. In August 2015, the courts sided with the FTC, opening the door for further enforcement of such standards.

This decision is of critical importance to companies. If such high-profile breaches have propelled the issue of cybersecurity to the top of the corporate agenda, the FTC decision has prompted some to evaluate—or reevaluate—how they address cyber liability.

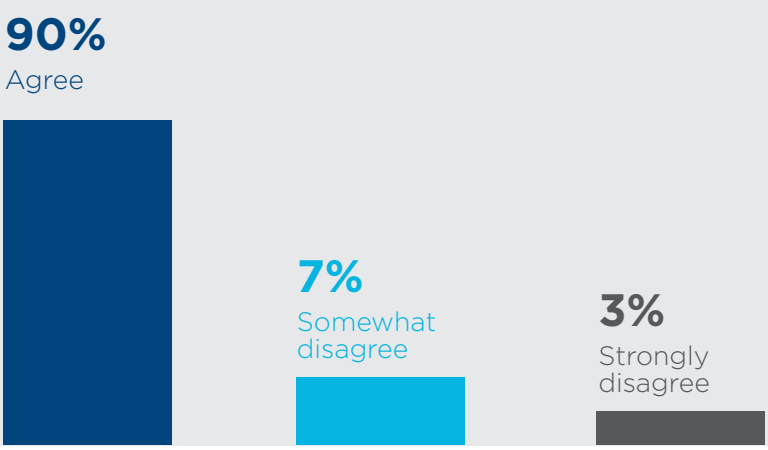
An increase in shareholder lawsuits is expected as a result of heightened corporate cybersecurity liability.

Demonstrating the seriousness of the issue, four out of five directors and officers stated they've brought the issue of cybersecurity liability to the forefront of their boardroom discussions. Even with this heightened scrutiny, three out of five directors and officers foresee an increase in shareholder lawsuits as a result of heightened corporate cybersecurity liability.

Moreover, more than half of our respondents believe investors will demand greater cyber-incident transparency from companies as a result of the increased public focus on cyber liability (Figure 3).

Consequently, boards would be wise to raise their games by disclosing more details of their oversight efforts and engaging with investors when cyber incidents occur, or they may run the risk of a loss of investor confidence[8].

FIGURE 2
How strongly do you agree that software providers should be held liable for breaches resulting from vulnerabilities found in their packaged software (applications, databases, libraries and frameworks, etc.)?



Businesses are ramping up for cyber-related regulation.

With 72% expecting more cyber-related regulation in the near future, most companies have begun intensifying their cyber risk management efforts. As a result of cyber liability concerns, 77% of respondents say they have already increased their security assessments, while an additional 17% report they are planning to do so in the near future.

Nevertheless, many companies are still only focusing on implementing the minimum set of controls required to demonstrate compliance with regulations, such as SOX, PCI DSS, and HIPAA. Yet, achieving compliance alone typically isn't sufficient to protect against other significant consequences of cyberattacks, such as theft of corporate intellectual property and revenue loss from system downtime, not unlike those experienced by Sony in 2014. This is because government and industry regulations are exclusively focused on protecting sensitive customer and financial data, rather than other corporate assets.

Survey respondents also indicated other changes they've made to avoid future cybersecurity liability, including increased audit committee and board-level oversight—a strategy that is in line with expert recommendations to report to the audit committee on a quarterly basis and to the full board annually.

Some directors and officers also say they are increasing security training for staff and hiring outside consultants. Boards can't neglect the added value of enlisting the help of third-party experts to train staff and independently verify the security of their networks and Web and mobile applications, whether internally developed or externally sourced. A well-prepared board that seeks to fulfill its fiduciary duty will not simply ask what happens "if" the company gets hacked, but rather how the perpetrators might get in, whether the company is doing all it can to reduce risk and prevent successful cyberattacks, and how it will respond if breached.

Businesses are turning to cybersecurity insurance as an additional means to mitigate cybersecurity liability.

The majority of companies utilize cybersecurity insurance as an additional means to mitigate financial losses brought forth by liability claims as a result of a cyber incident, whether the incident was spawned from the company's own systems or the use of vulnerable third-party applications.

Regardless of a company's size or industry, the threat of a cyberattack is so imminent that in an Oct. 12, 2015 article from Reuters, reporter Jim Finkle states that the cyber insurance market is set to triple to about $7.5 billion in the next five years[9].

According to the article, the price of cyber coverage, which helps cover costs like forensic investigations, credit monitoring, legal fees, and settlements, varies widely, depending on the strength of a company's security defenses. However, the overall trend is sharply up. Retailers and health insurers have been especially hard hit by the squeeze after high-profile breaches at Home Depot, Target, Anthem, and Premera Blue Cross.

The majority of businesses we surveyed did carry some form of cyber coverage. Out of those that currently purchase cyber insurance, almost all (91%) subscribe to business interruption and data restoration protection, and more than half (54%) have also chosen coverage for expense reimbursement (PCI fines, breach remediation/notification, extortion, etc.).

For a payout to occur, insurance companies will require that a company prove it had adequate measures in place to protect its data. A growing number of companies are therefore preparing for this contingency, with 52% subscribing to employee/insider threat liability coverage and more than a third (35%) seeking coverage against loss of sensitive data caused by software coding and human errors.

Cyber insurance policies aren't a fix-all solution, however. For one, while they may help reduce a company's financial liability risk, they do not *prevent* cyberattacks, and they are unlikely to cover the full financial impact of brand damage and loss in shareholder value. Typical policy providers require companies to disclose the existence of defense technologies (Do you have protective technologies in place?) and processes (Do you have a process for identifying and remediating software vulnerabilities?).

FIGURE 3
Do you believe increased cybersecurity liability for businesses will result in any of the following?

Companies will increase their focus and spending on cybersecurity controls and training	88%
It will spawn more cyber-related regulation	72%
Companies will increase their cybersecurity liability insurance purchase/coverage	68%
Shareholder suits will increase	61%
Investors will demand greater cyber-incident transparency	54%
Corporate boards will become more risk-averse	37%
It will have a chilling effect on M&A	7%

[1] Forrester Research, Top Security and Risk Priorities For The Business Technology Agenda, March 10, 2015, p.4 [Report cited: Anne Coughlan, Vidka Kamate, and Yi Qian, "Brand Value and Stock Markets: Evidence from Trademark Litigations," Kellogg School of Management at Northwestern University, February 2014 (http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2536672)

[2] http://www2.deloitte.com/content/dam/Deloitte/global/Documents/Governance-Risk-Compliance/gx_grc_Reputation@Risk%20survey%20report_FINAL.pdf

[3] http://www.nytimes.com/2014/08/06/technology/russian-gang-said-to-amass-more-than-a-billion-stolen-internet-credentials.html

[4] http://www.darkreading.com/attacks-breaches/15-year-old-arrested-for-talktalk-attack/d/d-id/1322836

[5] http://www.verizonenterprise.com/DBIR/2015/, p.15

[6] NYSE and Palo Alto Networks, Navigating the Digital Age: The Definitive Cybersecurity Guide for Directors and Officers, October 2015, p.55 [Report cited: Ponemon Inst., 2015 Cost of Data Breach Study: Global Analysis (May 2015), http://www-03.ibm.com/security/data-breach/]

[7] http://www.darkreading.com/perimeter/ruling-ftc-can-hold-wyndham-liable-for-data-breach/d/d-id/1321881

[8] NYSE and Palo Alto Networks, Navigating the Digital Age: The Definitive Cybersecurity Guide for Directors and Officers, October 2015, p. 32 (https://www.securityroundtable.org/wp-content/uploads/2015/09/Cybersecurity-9780996498203-no_marks.pdf

[9] http://www.reuters.com/article/2015/10/12/us-cybersecurity-insurance-insight-idUSKCN0S609M20151012?feedType=RSS&feedName=technologyNews