IN FEBRUARY 2013, **PRESIDENT OBAMA DECLARED** THAT THE "CYBER THREAT IS ONE OF THE MOST SERIOUS ECONOMIC AND NATIONAL SECURITY CHALLENGES WE FACE AS A NATION" AND THAT "AMERICA'S ECONOMIC PROSPERITY IN THE 21ST CENTURY WILL DEPEND ON CYBER SECURITY."

WILLIS FORTUNE 500 CYBER DISCLOSURE REPORT, 2013

I. OVERVIEW

In October of 2011, the U.S. Securities and Exchange Commission (SEC) issued guidance to U.S.-listed companies to provide extensive disclosure on their cyber exposures.[1] In so doing, the Commission recognized the increasing reliance of companies on cyber security and the concern over more frequent and severe cyber incidents. While remaining mindful that detailed disclosures could compromise a firm's cyber security by disclosing *too much* information to those seeking to infiltrate a firm's network security, the SEC sought to balance this concern against the need to provide to investors with material, meaningful information pertinent to the buying, holding, or selling of a company's stock. Most U.S. public companies began complying with the SEC's guidance in 2012.

We view the SEC's guidance as a game changer.[2] While it is clearly directed at U.S.-listed companies with securities filing obligations, those that invest or lend funds to private companies with similar business plans and like exposures are likely to begin requesting similar disclosures from non-listed U.S. organizations (private companies). And as money is invested globally, non-U.S. firms looking to understand the risks in their international portfolio and expand their holdings will be closely watching these disclosures for the lessons to be learned.

Because initially, companies had no blueprint or past history of disclosures to follow, we speculated that variation among companies, even within the same industry and the same global footprint, might be rife.

Willis

Willis decided to undertake a study of the cyber disclosures prompted by the SEC's guidance, believing that such a study might be of benefit to those making cyber exposure disclosures and those interested in discernible trends (or aberrations).

This report on the Willis Public Company Cyber Exposure Disclosure Study with a Focus on the Fortune 500 (Study) highlights three key disclosure areas in the SEC's guidance:

- The significance of the organization's cyber exposures and how these are qualified
- How the exposures are likely to manifest themselves
- What the company is doing to mitigate these risks.

II. KEY FINDINGS

Our study found that, as of April 2013, 85% of the Fortune 500 are following the SEC guidelines, providing some level of disclosure regarding cyber exposures.

36% DISCLOSED THAT THE RISK WAS "MATERIAL," "SERIOUS" OR USED A SIMILAR TERM TO DESCRIBE THEIR RISK. ONLY 2% (12 OUT OF 500 COMPANIES) USED A STRONGER TERM, SUCH AS "CRITICAL," TO DESCRIBE THEIR CYBER RISK, SUGGESTING THAT A FAILURE MIGHT IMPACT THE COMPANY'S CONTINUED EXISTENCE.

Close to 40% of companies either did not provide details on the size of their exposure or thought it sufficient to note that the risk would have an impact on the company without any further description of the extent of the impact.

Based on the SEC-suggested factors to be assessed in determining one's cyber exposure, the number of banks, insurance companies, internet companies, IT services companies, retailers and telecommunications companies within the Fortune 500 that consider the risk material or serious but ***not*** critical – or that failed to make any qualitative judgment on their risk at all – may be remarkable. However, viewing the exposure as immaterial may well be due to their size as some of these firms may believe that they have more than sufficient assets to deal with any threat that might arise..[3]

Whether or not the companies that have made disclosures have done so to the level requested by the SEC is debatable. The SEC was asking for information on the probability of cyber incidents occurring and their quantitative and qualitative magnitude, including the potential costs and other consequences resulting from misappropriation of assets or sensitive information, corruption of data or operational disruption. Some of this material is provided by some companies, but it would appear that the level of disclosure might fall short of the detail requested by the SEC.

COMPANIES THAT SAID THEY WERE EXPOSED TO CYBER RISK WERE SPECIFIC AS TO THE TYPE OF CYBER RISKS THEY ARE FACING 95% OF THE TIME.

THE **TOP THREE RISKS** IDENTIFIED BY THE FORTUNE 500 ARE:

1) LOSS OR THEFT OF CONFIDENTIAL INFORMATION: **65%**
2) LOSS OF REPUTATION: **50%**
3) DIRECT LOSS FROM MALICIOUS ACTS (HACKERS, VIRUSES ETC.): **48 %.**

THESE RISKS ARE CLOSELY FOLLOWED BY EXPOSURE TO LIABILITY FOR SYSTEM BREACHES OR FAILURES (40%).

III. SPECIFIC RISKS

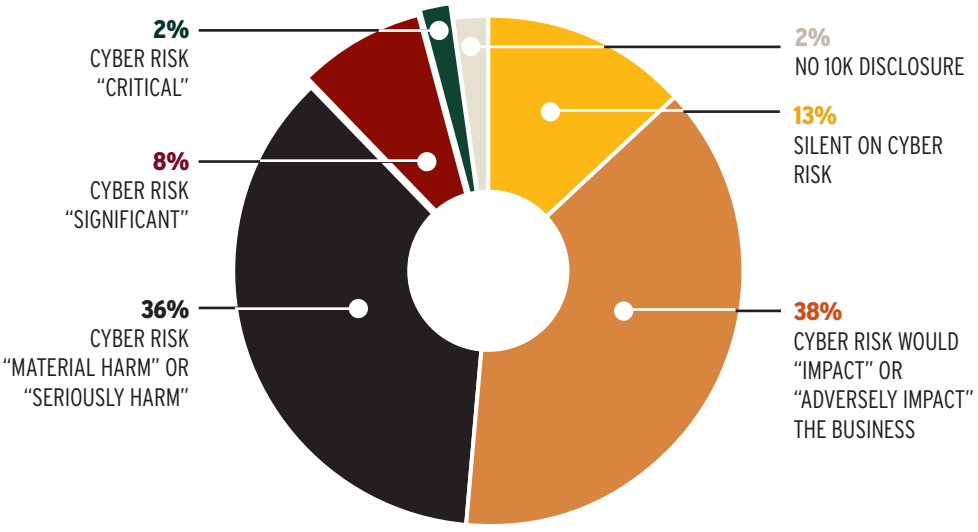
QUANTIFYING CYBER RISK

Our study found that:

- 38% disclosed that a potential cyber event might "impact" or "adversely impact" the business
- An additional 36% (180 companies of 500) may face "material harm" to their business due to cyber attacks
- 2% (12 companies) specified their potential cyber risk as "critical"

As reporting firms did not quantify their cyber exposures, we grouped them in order of significance from silent to critical. The results are displayed in the chart below.

EXTENT OF CYBER RISK



Our study found that 85% of the Fortune 500 are providing some level of disclosure regarding cyber exposures. Among those silent were insurance companies, a pharmaceutical company, a restaurant chain and a health care company – all of which appear to have some level of cyber risk when compared to the disclosures of their peers. In their cyber reporting Guidelines, the SEC suggested disclosing information on the probability of cyber incidents occurring and their quantitative and qualitative magnitude, including the potential costs and other consequences resulting from misappropriation of assets or sensitive information, corruption of data or operational disruption.

Over 50% of companies either did not mention the extent of the risk or merely noted that the risk would have an impact on the company without any further description of the extent of the impact. None of the companies provided actual dollar estimates of the impact of a cyber-security event, even though a reading of the SEC's guidance might lead one to expect them to do so.

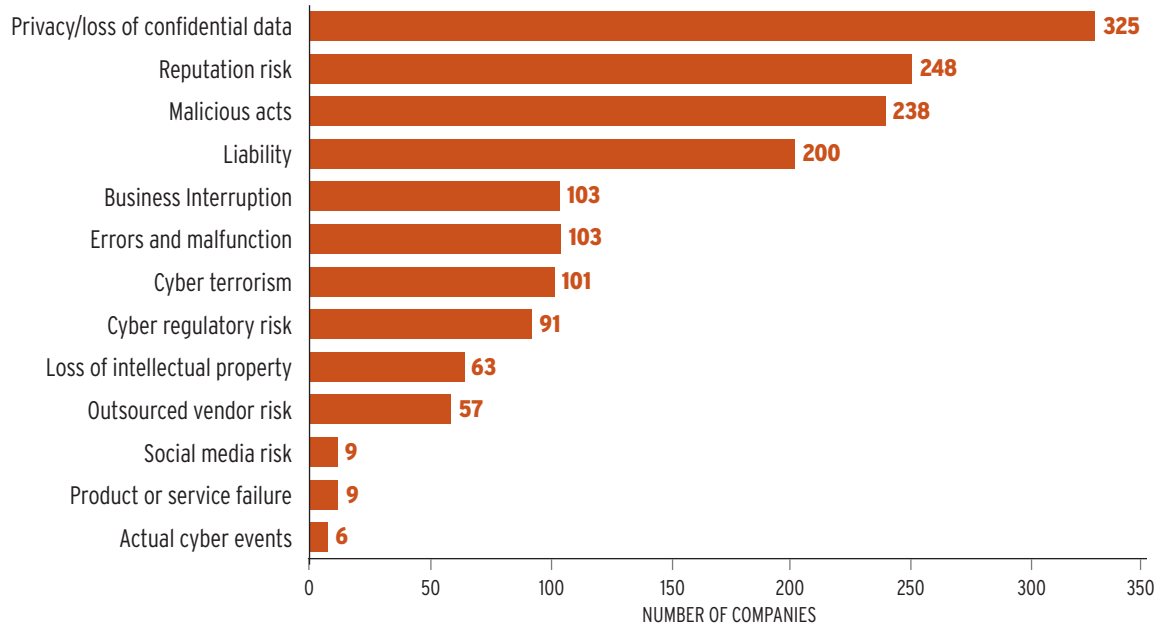
The few companies that used a term such as "critical" to describe their cyber risk seem not to have any particular relationship to one another (e.g., an auto manufacturer, a food and drink company, a distributor of petroleum products, two utilities, a large machinery manufacturer, a health care insurer, a life insurance company and a computer manufacturer).

EXPOSURES IDENTIFIED

The SEC asked that cyber security risk disclosure adequately describe the nature of the material risks and specify how each risk affects the firm, avoiding simply disclosing generic risk factors, and recommended that appropriate disclosures include:

- The aspects of the firm's business or operations that give rise to material cyber security risks and the potential costs and consequences
- Where outsourced functions have material cyber security risks, descriptions of those functions and how the company addresses those risks
- Risks related to cyber incidents that may remain undetected for an extended period
- Descriptions of cyber incidents experienced by the registrant that are individually, or in the aggregate, material, including the costs and other consequences

REPORTED EXPOSURES IN ORDER OF OCCURRENCE



Our Study found that companies that disclosed cyber risks were specific with respect to the types of risks they face 95% of the time. The top three risks identified, are:

1) Loss or theft of confidential information: 65%
2) Loss of reputation: 52%
3) Direct loss from malicious acts (hackers, viruses etc.): 50%.

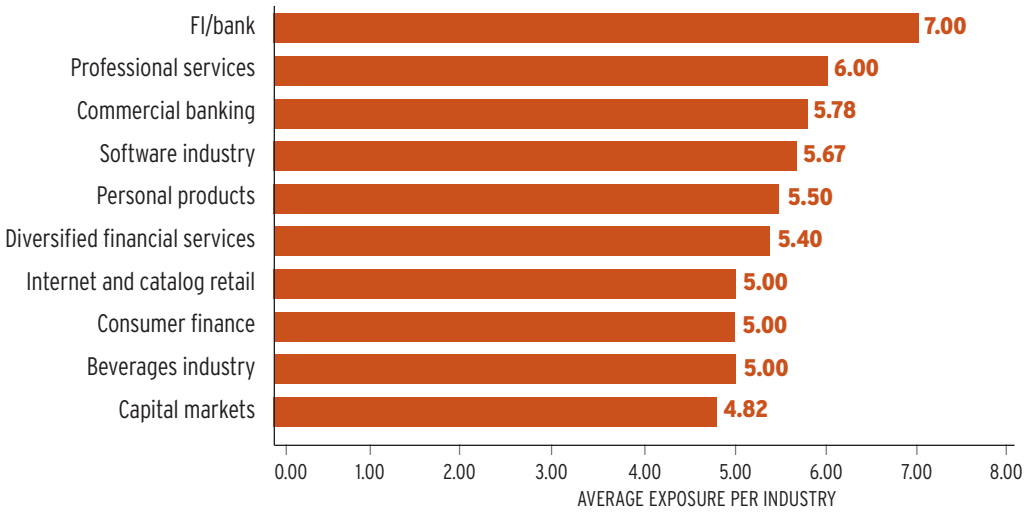
These risks are closely followed by exposure to liability for systems breaches or failures (40%)

Relatively few companies reported a potential cyber exposure related to loss of intellectual property (13%). Government sources have indicated that the federal government is particularly concerned about companies losing competitiveness to overseas entities that were stealing IP in the form of business plans, designs and products. Not surprisingly, many of the companies that identify this risk are in the defense, aerospace and technology sectors, but there is also a mix of the other industries. This will be considered more closely in our follow-on study by industry groupings [See: **V. Next Steps**].

Most companies in our study did not identify cyber terrorism as a risk; only 20% referred to it in the disclosure materials. However, industry groups where companies **did** specifically disclose cyber terrorism as a risk include many airlines and aerospace companies; utility, communications, media and insurance companies. This will be further discussed in our study where the disclosures are considered by industry classification [See: **V. Next Steps**].

The specifics requested by the SEC were mostly absent. Only five companies out of 500 or 1% disclosed an actual event. Even though 11% considered outsourced vendors to be a risk, many of the disclosures did not provide detail on the functions affected or how those risks are addressed. None mentioned the latent cyber risk or potential or actual costs of events in dollar terms, even though this is specifically requested in the SEC guidance.

TOP 10 AVERAGE RISK EXPOSURES PER INDUSTRY

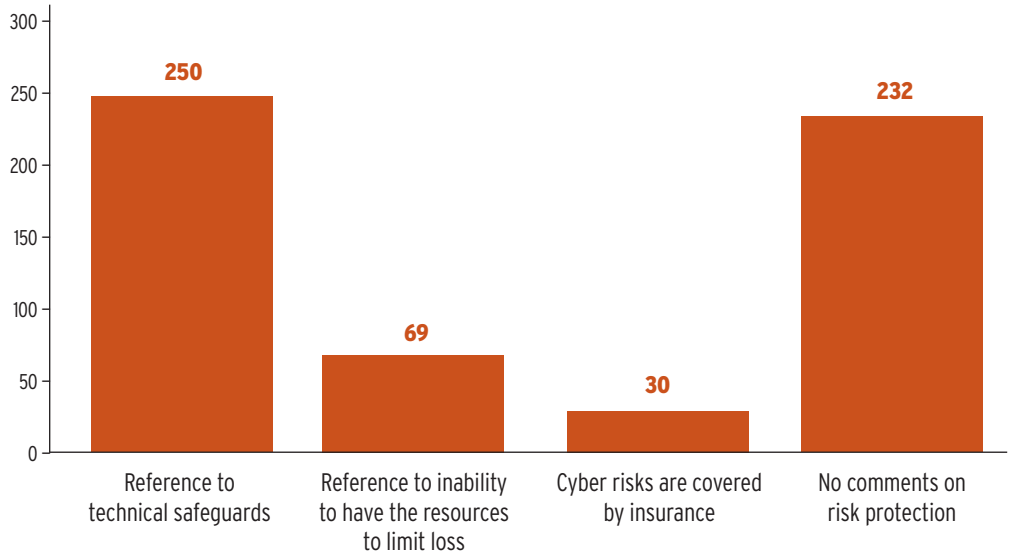


Industries that identified the most specific exposures are grouped in the financial and technology sectors of the economy. The industry groups represented at the lower end of the scale that we expected to see higher up in providing details of exposures include insurance, electric utilities and the hospitality industry.

PROTECTION AGAINST CYBER RISK

The SEC guidance requires that public companies disclose conclusions on the effectiveness of disclosure cyber controls and procedures and consider whether there are any deficiencies in its disclosure controls and procedures that would render them ineffective. Some commented on this point, but 46% declined to give any information at all.

RISK PROTECTION



The SEC guidance indicated that insurance of cyber risks may be an area appropriate to mention.[4] Only 6% of companies mentioned that they purchase insurance to cover cyber risks. This is inconsistent with recent surveys showing a much higher take-up rate for cyber insurance among public companies. A recent survey by Chubb for public companies[5] concludes that 35% of public companies purchase cyber insurance – even though they identify cyber risk as their number one concern. A quarter of those surveyed by Chubb are expecting a cyber breach in the coming year, and 71% have cyber breach response plans in place.

Less formal reviews by Willis' Cyber and E&O team reveal that, in some sectors, the rate of purchase of cyber insurance is above 50% for large public companies. Willis sees the take-up rate differing significantly by sector; some sectors are well below 10%.

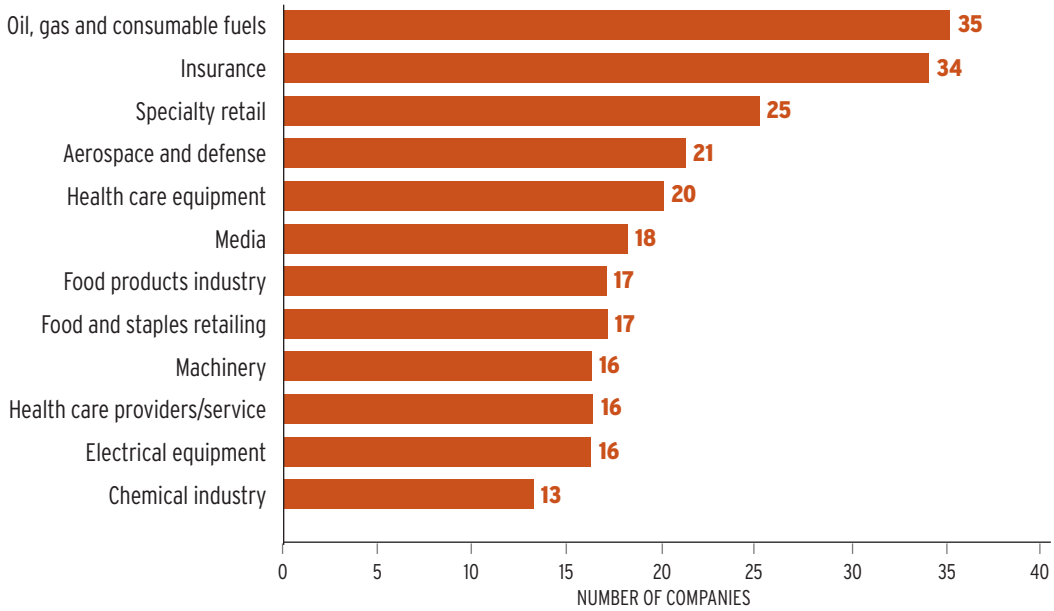
Companies that say they buy insurance to cover cyber risks are concentrated in the financial, media, utility and energy areas.

Many companies (52%) refer to technical solutions that they have in place, but a significant number (15%) indicate that they did not have the resources to protect themselves against critical attacks.

IV. METHODOLOGY

Our study, as mentioned, focused on the Fortune 500. We reviewed each 10(k) filed with the SEC, keying in their descriptions of exposures (if any).[6] A database was created of company-specific disclosures. The chart below displays the industry classes identified in the public filings.

INDUSTRY REPRESENTATION IN THE FORTUNE 500



V. NEXT STEPS

We have already begun work on a follow-on study, looking at the disclosures of select industry groups, including many of those identified by the U.S. government as "critical infrastructure." We also plan to examine the Fortune 1,000 to see if the results change when a larger pool of companies is considered.

As of this writing, the Senate is set to vote on passage of the Cyber Intelligence Sharing and Protection Act (CISPA), a law that would allow for the sharing of internet traffic information between the U.S. government and certain technology, manufacturing and utility companies to encourage the sharing of information. The bill's aim is to help the U.S government investigate cyber threats and ensure the security of networks against cyber attacks.[7]

Disclosure standards may also be evolving, although it is too soon to say if the SEC will react to recent requests to heighten the new disclosure recommendations.[8] Should standards change, future study would likely examine how companies then categorize and respond to cyber risks.

CONTACTS

For additional information, please contact your Willis Client Advocate® or **FINEX_NA@willis.com**.

For past issues of our publications on other topics of interest, please visit the **Executive Risks website**.

FINEX Alerts*, newsletters and white papers provide a general overview and discussion on a wide range of topics. They are not intended, and should not be used, as a substitute for legal advice in any specific situation.*

---

1 **http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm**.

2 See Willis Alert: *Radical New Cyber Exposure Disclosure Guidance for Public Companies*, November 2011, and our Willis Wire BLOG: *SEC Guidance on Cyber Attack Disclosure: A Game Changer?*

3 This may be true because larger companies have more resources to address and recover from a breach. Some of the smaller public companies (not included in this study focusing on the Fortune 500) mentioned having insufficient assets to weather a worst-case cyber-attack.

4 "Cyber security" refers to the technologies, processes and practices designed to protect networks, systems, computers, programs and data from attack, damage or unauthorized access. **http://www.merriam-webster.com/dictionary/cybersecurity**

5 Chubb 2012 Public Company Risk Survey: Cyber **http://www.chubb.com/businesses/csi/chubb15936.html**

6 A company's annual Form 10-K filing provides a comprehensive overview of the company's business and financial condition and includes audited financial statements. Similarly named, an annual report in a 10-K is usually distinct from the company's "annual report to shareholders," which a firm must send to its shareholders when it holds an annual meeting to elect directors. **http://www.sec.gov/answers/form10k.htm**

7 HR 3523. The bill specifies that information shared may not be used by an entity to gain an unfair competitive advantage and that no civil or criminal cause of action is permitted in federal or state court for sharing information or for decisions based on cyber threat information identified, obtained or shared under the bill.

8 SEC Urged to Give Stronger Guidance on Cyber Disclosure, Apr 10, 2013 9:57 AM ET, **http://www.bloomberg.com/news/2013-04-10/sec-urged-to-give-stronger-guidance-on-cyber-disclosure.html**