"Securing cyberspace is one of the most important and urgent challenges of our time. In light of the growing threat and the national security and economic ramifications of successful attacks against American businesses, it is essential that corporate leaders know their responsibility for managing and disclosing information security risk."[1]

– Letter from Senator John D. Rockefeller IV, et al. to Chairman, Securities and Exchange Commission, May 11, 2011

WILLIS FORTUNE 1000 CYBER DISCLOSURE REPORT

I. OVERVIEW

In this second in a series of reports examining U.S. public company cyber disclosures, Willis expands the scope of the review to include the Fortune 1000.

The earlier Willis Fortune 500 Cyber Disclosure Report reviewed the 10-Ks or annual reports filed by the Fortune 500 in 2012, the period immediately after the U.S. Securities and Exchange Commission (SEC) published its guidance that public companies might best include more extensive disclosures relating to their cyber exposures.[2]

The initial study addressed three important questions on the public disclosures of those companies:

1) The size or extent of the risk
2) The types of exposures identified
3) The steps being taken to reduce cyber risks

This updated study asks the same questions of the wider pool of companies and highlights industry groups.

The SEC's suggested guidance was that U.S. public companies include the nature of the risks and how each risk might affect the firm, recommending that these disclosures be unique and specific to each firm, not generic.

Quite a tall order for U.S. public companies ***and*** for the SEC, which reviewed, and in some cases commented on, the reports prior to releasing them to the public. Many of our largest public companies face interdependent exposures and were largely unable to review

Willis

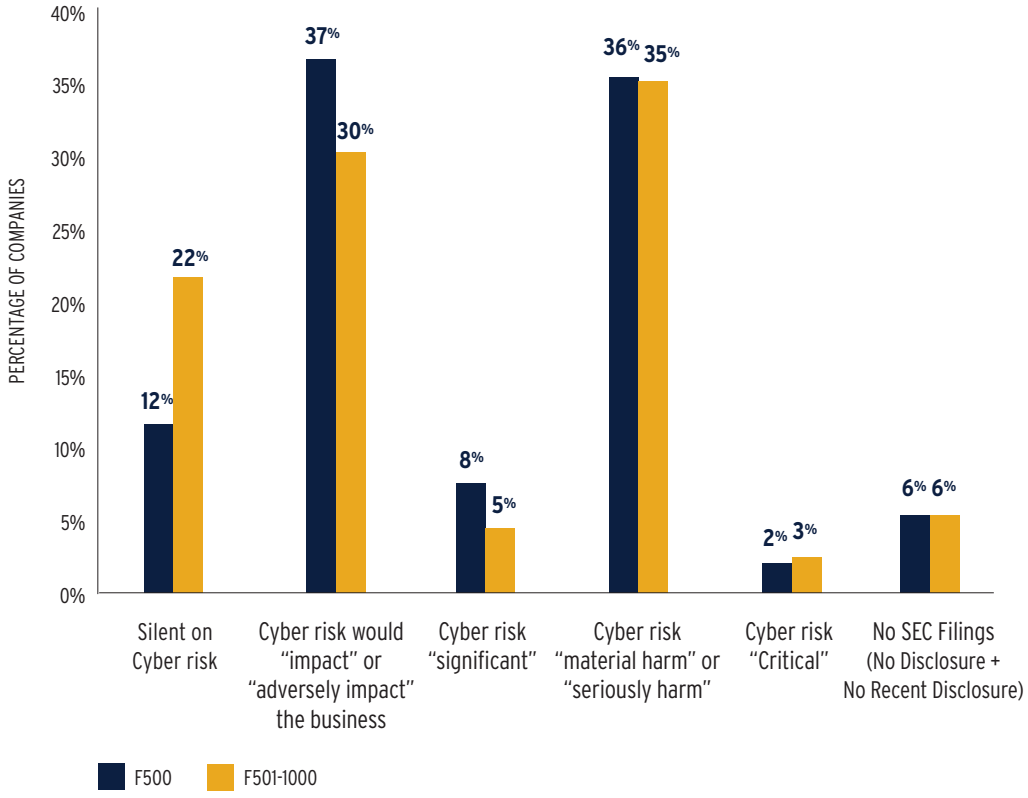
the disclosures of their trading partners and vendors at the time they were filing their own reports. Responding to the SEC's guidance for the first time had to have been a challenge.

II. BIG VERSUS BIGGER: COMPARING THE FORTUNE 501-1,000 TO THE FORTUNE 500

QUANTIFYING THE RISK

While there are significant differences in the industry makeup of the Fortune 500 and the Fortune 501 to 1,000, remarkable similarity exists between the two groups in their disclosures on the size or extent of their cyber exposures. The most significant difference we found was in the number of companies that remained silent on their cyber risk: 12% in the F500 segment was silent, compared to 22% in the F501-1000 (see Chart 1 below). The reason for this may be that, as companies get smaller, they may see themselves as less likely targets of an attack, or it may be that smaller companies needed more time to identify their cyber exposures.

CHART 1 **REPORTED EXTENT F500 v F501-1000**



While the SEC's guidance is just that, advice on what public companies might disclose, it comes from their Division of Corporation Finance – the division that selectively reviews public company securities filings to ensure compliance with relevant disclosure and accounting requirements. When they speak, public companies usually listen.

CYBER EXPOSURES IDENTIFIED

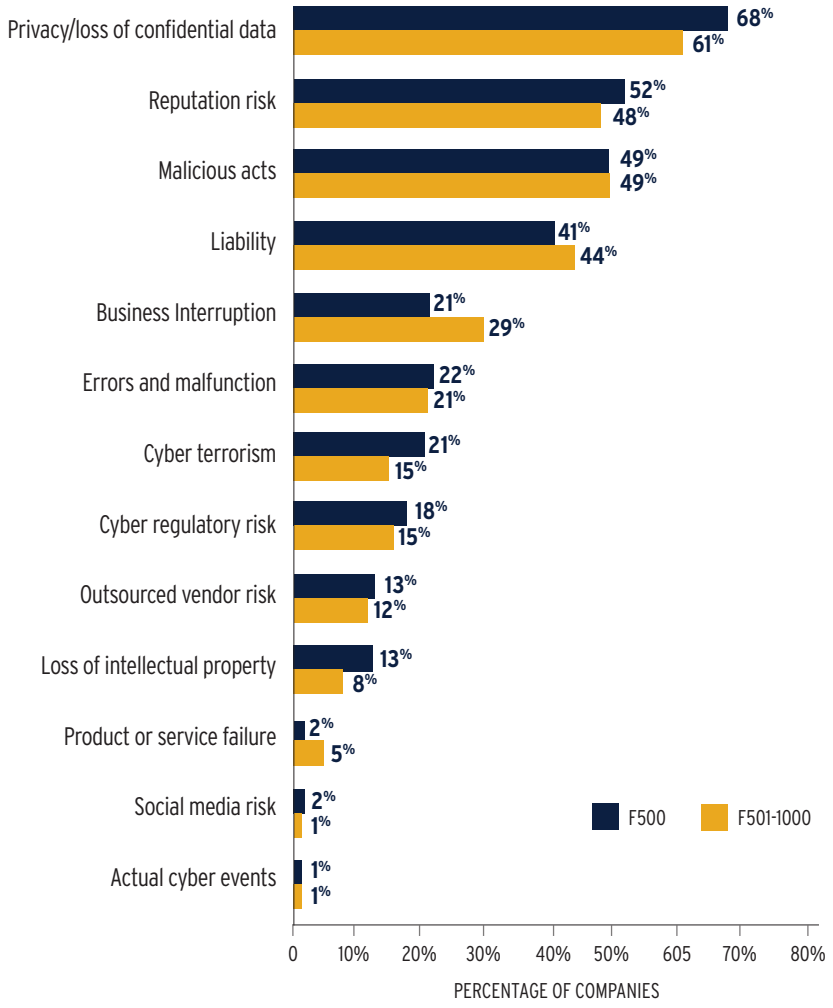
The companies in both the F500 and the F501-1000 groups used similar terms to explain the cyber exposures facing their organizations. The most significant differences between the two groups, as seen in Chart 2, are:

1) A rise in the exposure to business interruption as a result of a cyber event (from 21% for the F500 to 29% for the F501-1000)
2) A reduction in the perceived exposure to cyber terrorism (from 21% to 15%)
3) A reduction of intellectual property risks identified (from 13% to 8%)

For the Fortune 1,000, cyber terrorism and intellectual property risk disclosures are lower than we expected given the focus of the federal government on these areas of risk and their possible effects upon the health of the U.S. economy overall.

We note that the disclosure of actual cyber events remains at 1%, a seemingly low number given the number of attacks that appear in the press on a regular basis. Furthermore, even though the SEC guidance requests dollar costs of attacks that have occurred, none of the companies that disclosed actual attacks included the associated costs.

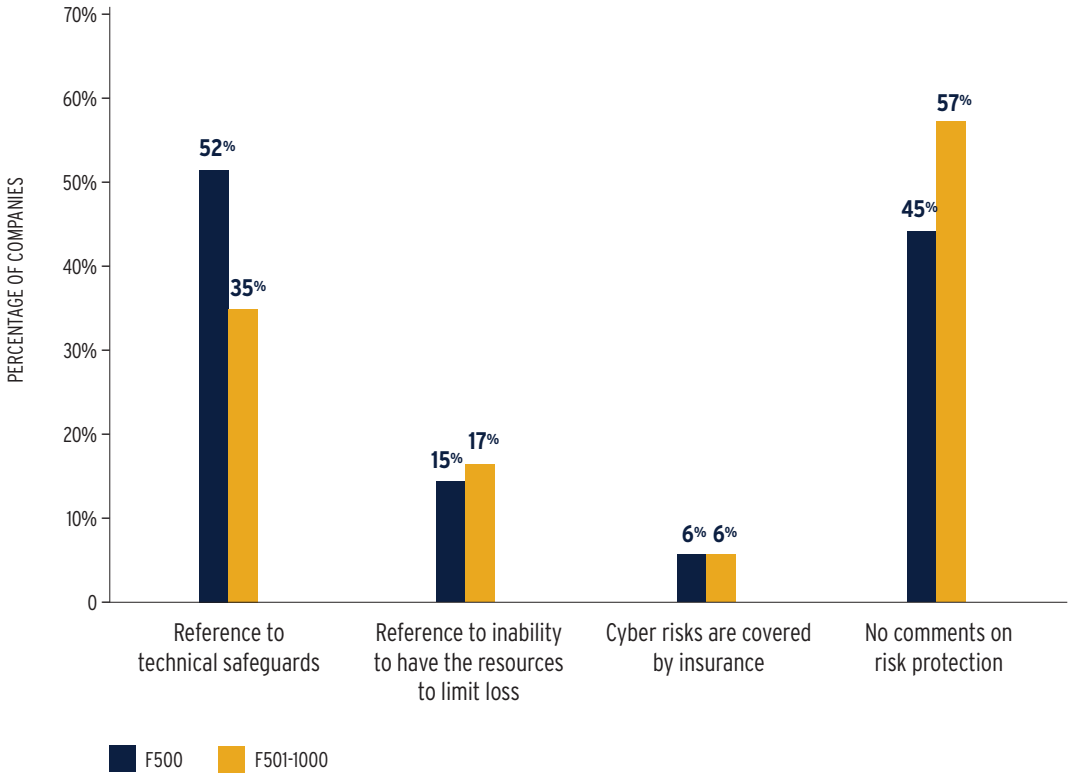
CHART 2 **REPORTED EXPOSURES F500 v F501-1000**



LOSS CONTROL: RISK PROTECTIONS

Another significant difference between the two groups is the major drop in the disclosed use of technical risk protections – such as firewalls, intrusion detection, encryption, etc. – mentioned by 52% of the F500 but only 35% of the F501 – 1000 (see Chart 3). The disclosure of insurance for cyber risk remains steady at 6% for both groups (see more below), but the numbers of companies that make no reference at all to the protections they have in place rose from 45% in the F500 to 57%. This may be attributable to the higher percentage of companies that are silent on the topic of cyber exposure in the F501-1000 group.

CHART 3 **REPORTED RISK MANAGEMENT F500 v F501-1000**



III. INDUSTRY FOCUS

Willis divided the Fortune 1,000 into 20 industry groups to compare the disclosure of each. In doing so we recognize that while all industries are important, not all are *critical*. In fact, the Presidential Policy Directive on Critical Infrastructure Security and Resilience has identified 16 essential industry sectors as critical infrastructure.[3] Most, but not all, are included in our industry focus on the Fortune 1,000.[4]

Among those critical sectors, some are hyper-critical, such as the technology and telecom sector – since it serves an "enabling function" across all other critical infrastructure sectors.[5] Others are both critical and highly interdependent – such as the health care sector, where

collaboration and information sharing between the public and private sectors is essential ***and*** which is highly dependent on other industry sectors for continuity of operations and service delivery.[6]

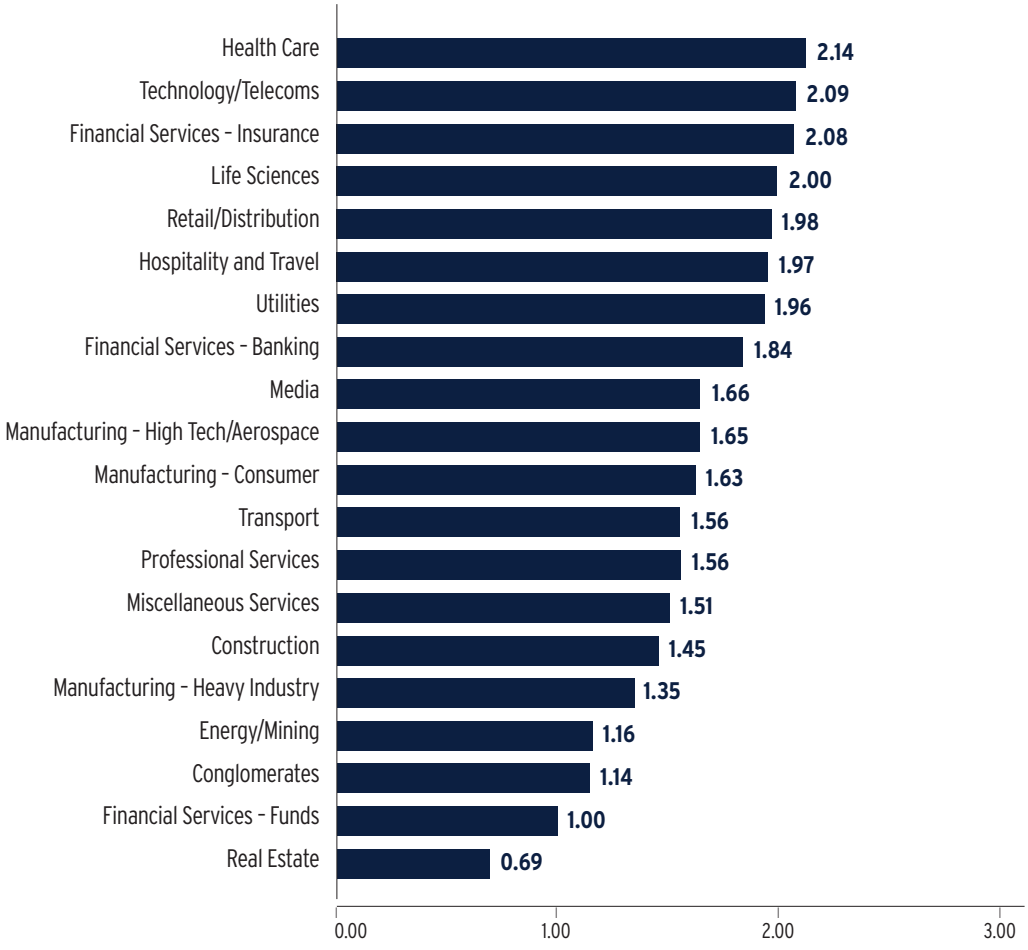
In our industry focus, we addressed the same questions as we did in our original study on the Fortune 500: 1) the size or extent of risk, 2) how the exposure would manifest and 3) what protections were being employed.

To measure the level of concern of each industry, Willis assigned a score for the extent of cyber risk each company disclosed. Using this score, health care is the industry most concerned about cyber risks, closely followed by the technology, insurance, telecom and retail sectors (see Chart 4). The sectors that disclosed the least level of concern are real estate and, perhaps more surprisingly, financial services-funds, conglomerates and the energy and mining sectors.

EXTENT OF THE RISK – BY INDUSTRY

There are significant differences in the disclosures involving the size or extent of the cyber risk faced by different industries in the F1000. Some of the variation may be as a result of the small number of companies in some industry groups but clearly, some industries are more exposed to the issue than others.[7]

CHART 4 **FORTUNE 1000 – INDUSTRY POINT SCORE – EXTENT OF RISK**

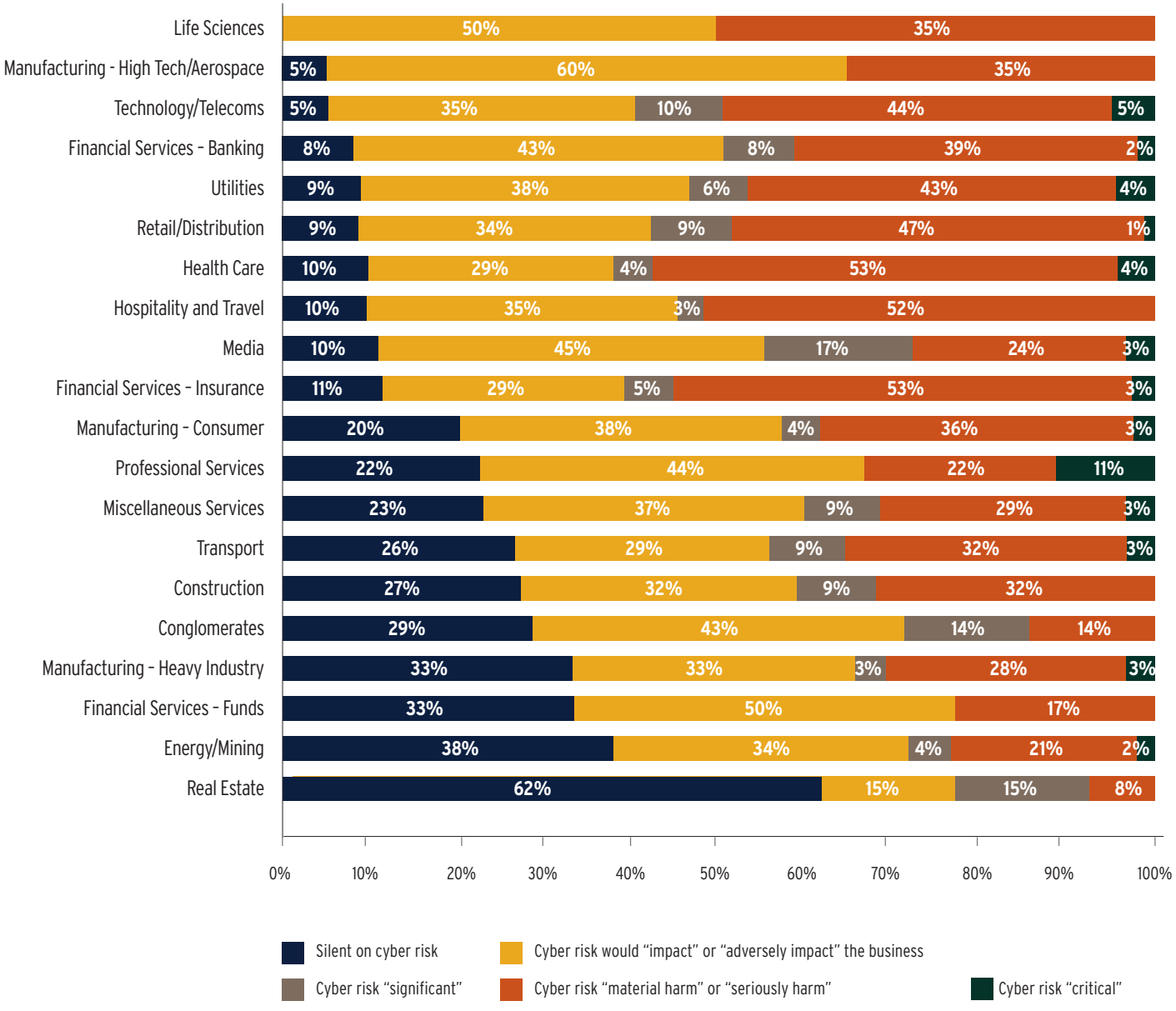


Industries that are naturally more reliant on technology and open networks such as banking, technology, aerospace, health care and utilities are more likely to disclose "significant" or "material impact" as the likely result of a cyber event (see Chart 5 below).

The limited number of companies that describe their exposure to a cyber event as "critical" are scattered throughout the industry sectors with professional services firms standing out as the sector that most often describes the exposure as critical, with 11% of the industry putting cyber risk in that category. Otherwise, there is no discernible pattern among companies or groups that note the risk as "critical."

- 62% of real estate companies did not have any comment on cyber risk
- 38% of the energy and mining sector remained silent as to cyber exposure

CHART 5 **FORTUNE 1000 – EXTENT OF LOSS BY INDUSTRY**

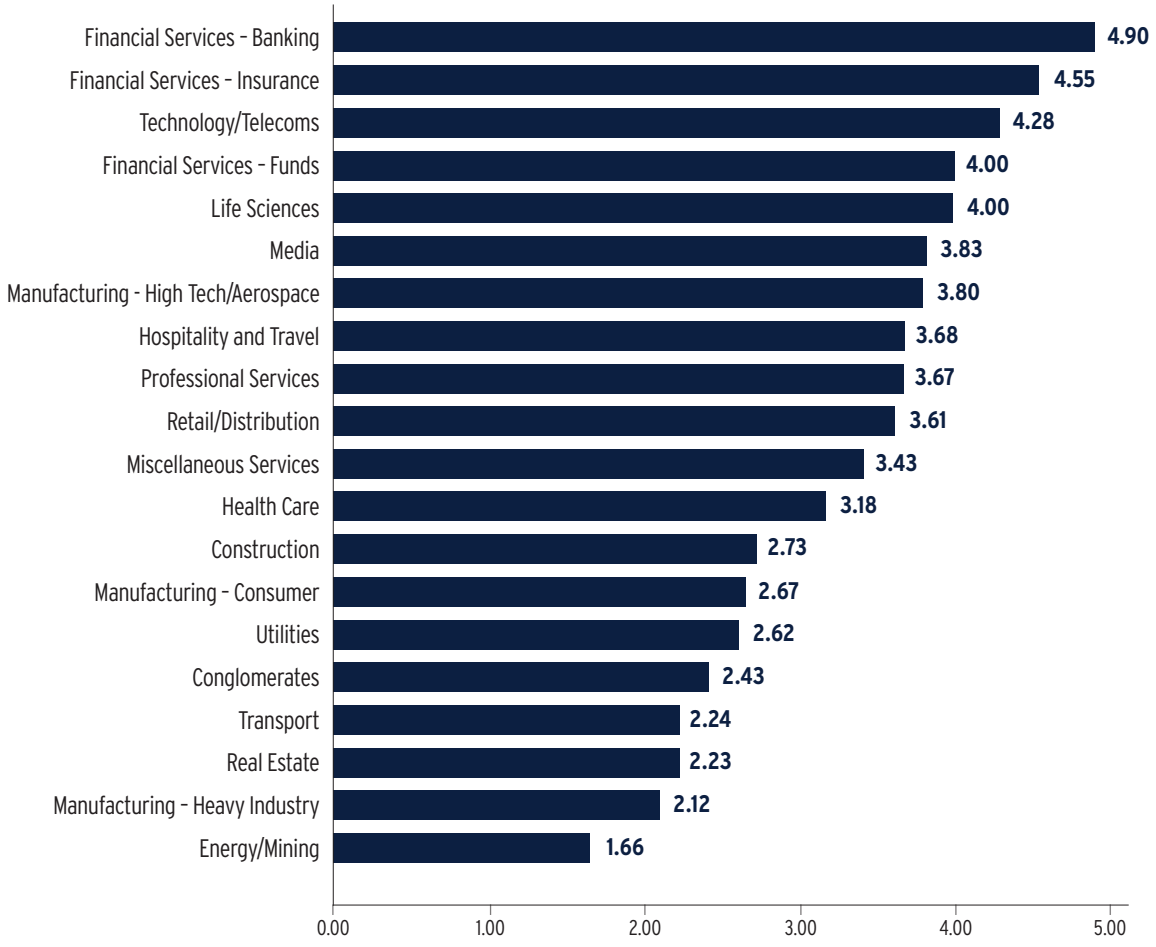


CYBER RISK EXPOSURES – BY INDUSTRY

To provide a different perspective, we totaled the number of different types of risks that companies disclose in their 10-Ks and averaged them for each. Looked at it this way, financial institutions and technology companies rise to the top of the list with the banking sector disclosing an average of 4.90 distinct cyber exposures (see Chart 6).

Interestingly, funds companies, featured at the low end of the scale when describing the extent of their cyber risk exposure, are close to the top of the chart when it comes to describing the number of different types of cyber risks that they face. While the small number of companies in the funds group (3) may account for the discrepancy, the difference may be due to a level of caution in an industry that is risk-management focused but does not have a large exposure to personally identifiable information, which is usually kept at the retail investment company level.

CHART 6 **FORTUNE 1000 INDUSTRIES – NUMBER OF EXPOSURES DISCLOSED**

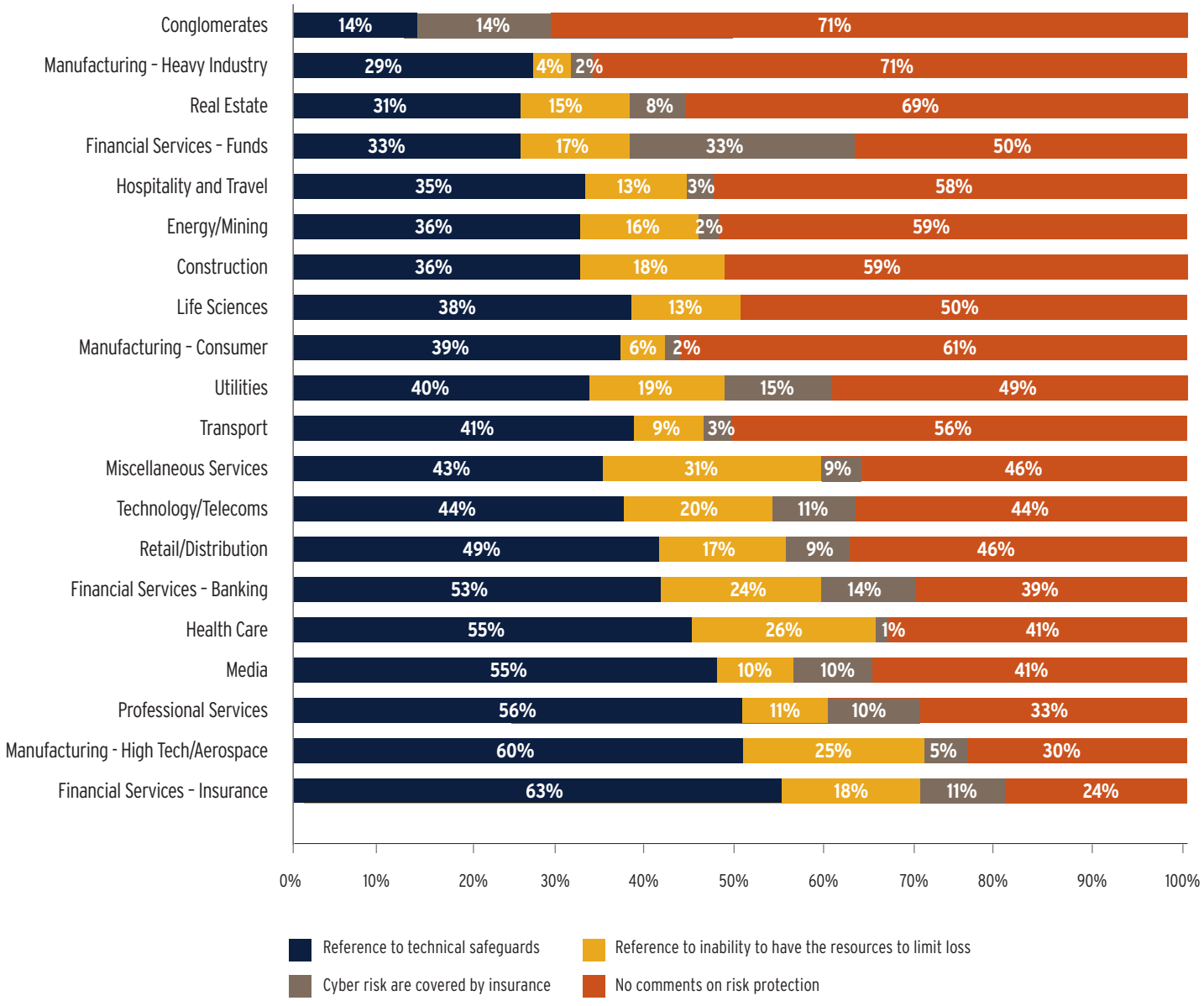


Industries at the lower end of the chart (reporting fewer exposures) include energy and utilities. Surprising, given that both have been identified as critical to the economy and covered in the press as objects of cyber attacks.

LOSS CONTROL – BY INDUSTRY

The industry groups that disclosed the greatest number of technical protections against cyber risk (firewalls, intrusion detection, encryption etc.) are the technology, health care, professional services and financial institution sectors with the insurance industry in the lead (see Chart 7). **Insurance companies refer to technical risk protections 63% of the time.**

CHART 7 **FORTUNE 1000 – RISK PROTECTION (%)**



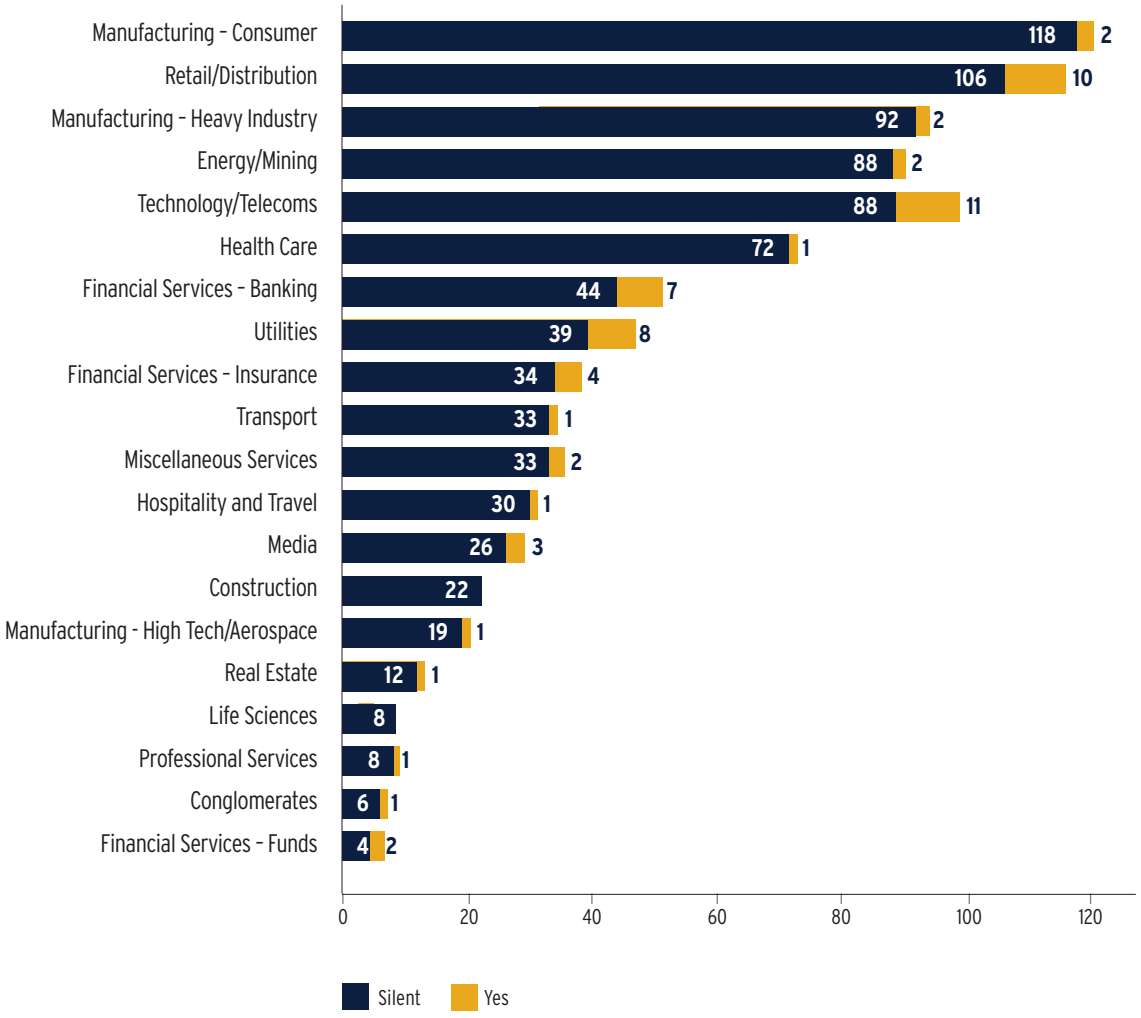
The industries within the Fortune 1,000 that most frequently state they have insufficient resources to limit the consequences of a cyber attack are miscellaneous services (31%)[7], health care (26%), high tech/aerospace (25%) and banking (24%). As the Fortune 1,000 includes the very largest U.S. public companies, this may be a serious concern.

LOSS PROTECTION – INSURANCE

The industries in our study that disclose they have the greatest level of insurance of cyber risks for their sectors are the funds sector (33%), followed by utilities (15%), the banking sector and conglomerates (14%). The insurance and the technology sectors both disclose the purchase of insurance covering cyber risk at the 11% level (see Chart 8 below).

A recent informal survey of life and health insurance companies conducted by Willis and key cyber insurance underwriters found that in the F1000, more that 60% of this sector purchased stand-alone cyber coverage. Willis concludes that many companies may be under-reporting insurance covering cyber risks. In our experience, the health care sector has been one of the largest purchasers of stand-alone cyber insurance, but only 1% of the industry mentioned purchasing it in their 10-Ks.

CHART 8 **INSURANCE COVERAGE – NUMBER OF COMPANIES**



DETAILS PLEASE

In its guidance, the SEC suggested that U.S. public companies include a level of detail not previously seen in most public company disclosures. They suggested disclosure on:

- The aspects of the firm's business or operations that might give rise to material cybersecurity risks and the related potential costs and consequences
- Where outsourced functions have material cybersecurity 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
- Disclosure of cyber incidents experienced by the firm that individually, or in the aggregate, are material, including the costs and other consequences
- Description of relevant insurance coverage

As our report reveals, during the first wave of disclosures after the SEC's guidance, there was a range of responses, even from companies of the same size in the same industry.

Examples of the range of cyber disclosures:[9]

EXAMPLE #1

Risks facing the company might arise from...the failure to adequately maintain security and prevent unauthorized access to electronic and other confidential information and data breaches could materially adversely affect our financial condition and operating results.

The firm has become increasingly centralized and dependent upon automated IT processes. Furthermore, a portion of our business is done over the Internet, increasing the risk of viruses that could cause system failures and disruptions of operations. A failure to maintain the security of our customers' confidential information, or data belonging to ourselves or our suppliers, could put us at a competitive disadvantage, result in deterioration in our customers' confidence in us, and subject us to potential litigation, liability, fines and penalties, resulting in a possible material adverse impact on our financial condition and results of operations.

Our computers and those of our suppliers are vulnerable to interruption by fire, natural disaster, power loss, telecommunications failure, terrorist attacks and acts of war, Internet failures, computer viruses and cyber attacks. The occurrence of any of these events could significantly disrupt our operations or result in a significant interruption in the delivery of our good and services which might harm our reputation and lead to the loss of some of our existing customers as well as impact our ability to compete for new business...

EXAMPLE #2

Risks include...the impact on the firm's locations and operations due to a terrorist attack, cybersecurity threats and other catastrophic events...

During the first round of financial reporting, companies failing to meet the level of disclosure deemed sufficient by the SEC might receive a comment letter from the agency – as has happened to approximately 50 public companies – asking them to supplement or amend their filings where appropriate. **http://blog.willis.com/2013/06/cyber-disclosures-of-the-fortune-500-how-companies-rate-their-cyber-exposure-for-the-sec/**

OUTSOURCED VENDORS AND THE CLOUD

One of the key areas that the SEC asked companies to address, both in its original guidance and in its subsequent comment letter, was the potential risk represented by outsourced vendors. The request seems particularly apt in the context of the balancing act that IT departments have to maintain between the costs and benefits of using the "cloud" and outsourced vendors against the risks of having information and operations in the hands of third parties. The exposure may be heightened by the fact that most technology service contracts severely limit the ability of companies to recover against vendors after a breach or failure of systems.

> Cloud computing [is] a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.[10]
>
> – The National Institute of Standards and Technology

Remarkably, only 13% of the companies in the F500 and 12% of companies in the F501-1000 mention vendor risk. When they do, the disclosure usually simply mention that the risk exists, but then fails to delve into the functions of the company that may be affected if the outsourced vendors are breached.

IV. THE FUTURE

ACTION BY THE FEDERAL GOVERNMENT'S EXECUTIVE BRANCH

On February 12, 2013, President Obama signed a new Executive Order entitled "Improving Critical Infrastructure Cybersecurity" which authorizes the dissemination of cyber intelligence reports to owners and operators of certain enterprises.[11] It also directs the collaborative development and implementation of risk-based cybersecurity standards. Recent news from the White House indicates that the administration and the Department of Homeland Security (DHS) are considering tax breaks, insurance perks (so far unidentified) and other legal benefits for businesses that make meaningful improvements to their digital defenses.[12]

Two types of cyber intelligence can be delivered to companies:

(1) Reports of cyber threats to the U.S. homeland that identify a specific targeted entity

(2) Reports which identify critical infrastructure "where a Cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security."

It appears that any company that receives a DHS report is on notice that the DHS expects the company to reinforce their resilience to cyber attacks, develop capabilities for informing themselves on when and where an attack may occur and managing the crises. Access to intelligence reports may be a two-edged sword.

CURRENT ACTION BY THE OF THE FEDERAL GOVERNMENT (SEC)

SEC Chairman Mary Jo White recently asked her staff to evaluate the SEC's current guidance for cybersecurity disclosures and to consider whether more stringent requirements are necessary.[13] Senator Jay Rockefeller, who has encouraged the SEC to provide further guidance on cybersecurity disclosures and was at the forefront of the SEC's initial guidance,[14] was told in the letter, dated May 1, that the SEC Chair believes that the initial guidance to companies on cybersecurity "has had a positive impact" on better informing the stakeholders of public companies.[15] Our study on the initial response by the largest U.S. public companies seems to confirm this while suggesting that some improvements may be possible.

V. NEXT STEPS

Action taken at the federal level clearly shows that cybersecurity disclosure by public companies is high on the federal agenda and will continue to pose a unique challenge for public companies. Government authorities may require companies to step out of their comfort zone for disclosures in order to bolster IT security for the entire U.S., opening up greater liability to directors and officers in the process. To protect themselves, companies may want to be more open and detailed in the way that they describe cyber risks in their public documents; but this could also play against them if they reveal a large exposure and only limited resources to protect themselves.

Meanwhile, we are working on a series of separate, more in-depth industry profiles on the unique cyber disclosures of the Fortune 1,000.

---

1 **http://commerce.senate.gov/public/?a=Files.Serve&File_id=4ceb6c11-b613-4e21-92c7-a8e1dd5a707e**

2 Securities and Exchange Commission, CF DisclosuF Disclosure Guidance, Topic No. 2: Cybersecurity, October 13, 2011 , **http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm**

3 **http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil**, February 12, 2013.

4 Critical infrastructure sectors such as the government facilities sector and commercial facilities sector are two examples of sectors not well represented (or present at all) in the Fortune 1,000.

5 **http://www.dhs.gov/communications-sector**

6 **http://www.dhs.gov/healthcare-and-public-health-sector**

7 E.g., there are only eight companies in the life sciences group, all of which disclose some level of cyber risk.

8 This is concerning as the group includes many non-tech vendors for large corporations.

9 Please note that these examples have been modified from actual disclosures.

10 **http://info.apps.gov/content/what-cloud**

11 **http://www.politico.com/story/2013/07/white-house-considers-breaks-for-boosting-cybersecurity-94528.html**

12 Incentives to Support Adoption of the Cybersecurity Framework at **http://m.whitehouse.gov/blog/2013/08/06incentives-support-adoption-cybersecurity-framework**

13 *SEC Chairman Reviewing Company Cybersecurity Disclosures*, May 13, 2013 3:01 PM ET, **http://www.bloomberg.com/news/2013-05-13/sec-chairman-reviewing-company-cybersecurity-disclosures.html**

14 **http://www.rockefeller.senate.gov/public/index.cfm/press-releases?ID=134e9dd2-9b6c-49c2-bcff-073019bcd247**

15 "SEC Head Orders Review Of Cyberthreat Disclosure Guidance," May 14, 2013 **http://www.law360.com/articles/441415/sec-head-orders-review-of-cyberthreat-disclosure-guidance**