

Center for American Progress



New Strategies to Protect America: A Market-Based Approach to Private Sector Security

Robert Housman

and

Timothy Olson



HOMELAND SECURITY

Progressive Ideas for a Strong, Just, and Free America

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
WASHINGTON D.C. 20549

FORM 10-K
(Mark One)

New Strategies to
Protect America:
A Market-Based Approach to
Private Sector Security

Robert Housman and Timothy Olson

Securities registered pursuant to Section 12(g) of the Act:
Common stock, \$0.0001 par value; preferred share purchase rights;
Contractual contingent payment rights
(Title of class)

Indicate by check mark whether the registrant (1) has filed all reports required to be filed by Section 13 or 15(d) of the Securities Exchange Act of 1934 during the preceding 12 months (or for such shorter period that the registrant was required to file such reports), and (2) has been subject to such filing requirements for the past 90 days. Yes No

Indicate by check mark whether the registrant is an accelerated filer.

0

(Number of shares of common stock outstanding as of February 13, 2005)

Disclaimers:

- This report does not constitute specific legal advice or opinion with respect to any of the companies or filings discussed herein.
- This report analyzes select SEC filings from a sample of public companies. It is not intended to be a comprehensive analysis of any one company or industrial sector.
- In order to analyze the disclosure of potentially material security issues by public companies, this report utilizes both official and unofficial third-party reports on security at companies and within various sectors. The accuracy of some of these analyses has been challenged by other experts and critics. We rely on these reports not for their ultimate accuracy, but rather to raise the sorts of issues that corporate reports should be raising and addressing directly.

Introduction

Approximately 90 percent of America’s critical infrastructure is owned by the private sector. This infrastructure is vital to the security and health—economic, social and cultural—of the United States. Pipelines, electrical lines, water systems, communications infrastructure, broadcast companies, financial markets and gathering places such as stadiums, malls, theme parks, hotels and office buildings are all privately held. As then-Homeland Security Secretary Tom Ridge aptly stated, “We are a target-rich environment, and the private sector owns most of the targets.”¹

Our nation’s dependence on the private sector is not lost upon the terrorists that seek to do us harm. Osama bin Laden stated that the Twin Towers were selected because they were symbolic of American economic power.¹ Since 9-11, bin Laden has called upon al Qaeda to attack the American economy and the critical infrastructure that supports our way of life.

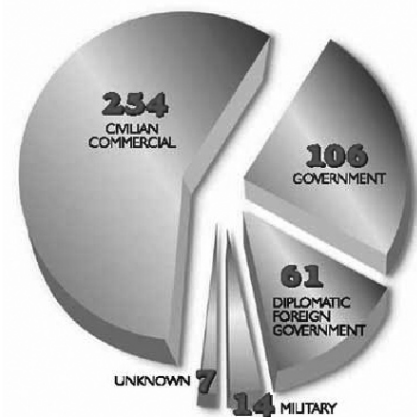
Even prior to 9-11, there was a growing understanding within national security circles that the nation’s critical infrastructure needed to be better protected. In 1998, President Clinton issued Presidential Decision Directive 63, entitled “Protecting America’s Critical Infrastructure.” It recognized the need to work with the private sector to improve the nation’s security from terrorism and other asymmetrical threats. However, the directive lacked the force of law, which limited its impact to better coordination and exchange of information between public authorities and private sector critical infrastructure owners. The main thrust of PDD 63 was cyber-security and not “brick and mortar” infrastructure.²

The attacks of 9-11, however, made it abundantly clear that still more needed to be done to protect critical infrastructure. In response, the Congress has passed legislation intended to better secure the nation’s infrastructure against terrorism.

The USA PATRIOT Act includes a number of commonsense provisions on critical infrastructure protection, particularly the financial services industry. The Aviation and Transportation Security Act federalized security at the nation’s airports and established new security rules for the airlines. The Maritime Transportation Security Act, and its implementing regulations, imposed new security requirements for thousands of “maritime facilities” around the nation—facilities ranging from cruise ship terminals to refineries located on U.S. waters.

The Terrorism Risk Insurance Act (TRIA) required insurers to offer terrorism risk insurance at terms not materially different from those offered for other categories of insured risk and set up a federal “backstop” for the property and casualty insurance market. Title IV of the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 established new security mandates for the nation’s drinking water systems.

Almost five years after the 9-11 attacks, we do not have a coherent and logical critical infrastructure protection system. For example, enhanced security provisions apply to the ships that carry hazardous chemicals and drivers of trucks that haul



Terrorist Activity by Target, 1998-2001; FBI

hazardous chemicals, but not to the chemical plants that store, use and manufacture them in bulk. Enhanced security mandates apply to the airline industry, but not rail systems that similarly carry millions of passengers each year.

Unfortunately, these developments have not sufficiently changed corporate security strategies. Plans have yet to go beyond the “Four G’s”—guards guns, gates and gadgets—and into the C-Suite and Board Room. They have not even reached the same breadth and depth as environmental mandates.³

In some sectors security has been greatly increased and is now more intrinsic to business operations and decision-making. However, a dangerous pre-9-11 complacency is returning. For example, in August 2004, New York’s financial institutions were placed on orange alert, but little changed in key financial centers elsewhere in the country.⁴ The threat was greeted with little more than a yawn by the sector as a whole and by all the other interdependent sectors.

Two surveys by the Conference Board, a non-partisan, not-for-profit business research organization, underscore this corporate complacency. One study indicated that between October 2002 and February 2003, the median increase in total security spending by major corporations was only 4 percent.⁵ The second Conference Board report determined that in 26 percent of companies surveyed, the CEO had not met with the security director at any time during the previous year.⁶

Other studies show that regular security meetings among corporate leadership have a direct bearing on security spending.⁷ Forty-five percent of the companies surveyed said they had not increased their spending since the 9-11 attacks.⁸ Remarkably, 1 percent of the companies surveyed had actually cut back on security spending. In other words, security is simply not viewed as a core business function. The Civitas Group, an investment firm that monitors the homeland security market estimated private sector homeland security spending would reach between six and seven billion dollars in 2005.⁹ This is a significant sum, but not all that much in a twelve trillion dollar (GDP) economy.

But from the private sector’s standpoint, this complacency is entirely rational:

- Global markets are highly competitive and companies are under extreme cost-cutting pressure. An American company that faces substantially higher security costs than a foreign competitor is potentially at a significant comparative disadvantage.
- In today’s just-in-time markets, anything that delays a company’s operations is seen as counter-competitive.
- The United States has enjoyed four years without another significant terrorist attack on our homeland. False alarms have created a proverbial “Chicken Little” dilemma.
- Political leaders tell the private sector that we are at war and that they are on the frontlines. However, many of the same political leaders are unwilling to place security burdens even on companies that may present the greatest risks.
- The risk of an attack against any particular company is uncertain and perceived as small.

The economic bleeding is continuing to date, but it requires further strikes. The young people should make an effort to look for the key pillars of the U.S. economy. The key pillars of the enemy should be struck, God willing.”

Osama bin Laden, Dec 27, 2001

However, while the likelihood of an attack against any specific company may be relatively small, the likelihood of an attack against this nation and its critical infrastructure companies is high. In other words, one could argue that critical infrastructure companies are betting their security on the roll of a dice that is—by virtue of what they do—loaded against them. Ongoing military efforts may reduce the ability of terrorists to conduct operations. However, as last year’s London attacks demonstrate, the threat remains.

While this complacency is understandable, it is not in the best interests of the nation, the American economy or shareholders.

What can the federal government do to enhance private sector security? What incentives, disincentives, mandates or other interventions can increase the importance of critical infrastructure security in corporate boardrooms? This report examines, in particular, disclosures under securities laws, rules, regulations and practice as a market-based measure for strengthening critical infrastructure homeland security. It then examines ways in which the Securities and Exchange Commission could encourage or compel companies to provide shareholders and the public with better homeland security information. It also provides select recommendations to companies regarding homeland security governance and disclosure issues to put more security in securities.

Strengthening Critical Infrastructure Security

There are three classes of governmental intervention that could play a role in meeting the goal of reversing private sector complacency regarding security:¹⁰

1. Impose standards: The government through laws and regulations could tell the private sector what types of security improvements are necessary.
2. Provide direct subsidies and/or incentives: The government could simply offset the costs of whatever security improvements are deemed necessary, such as via grants or tax incentives.
3. Establish market-based measures: Market-based measures enable companies to more efficiently allocate resources, correct market failures, eliminate free-riders and add weight to corporate security actions.

Each of these forms of intervention has advantages and disadvantages. Regulatory programs can impose higher and unnecessary costs and freeze innovation. Regarding direct subsidies, government simply cannot fund security improvements at all critical infrastructure facilities around the nation. Too much government influence might put critical business decisions and judgment into the hands of

Homeland Security and Shareholder Value

While Securities rules are increasingly seen as a public policy tool, at base, their purpose is to protect the investor. However, there are strong shareholder value reasons for the use of Securities rules to drive better more effective private sector homeland security:

1. A company that cannot secure its operations faces the likelihood of greater losses from not just terrorists, but also crime and natural disaster. For example, the Australian Institute of Criminology estimated in 2001 that global transportation supply chain losses total more than \$30 billion per year and are growing.*

2. A company that suffers a significant loss to terrorism, crime or disaster stands to lose customers and business goodwill. For example, a communications or power company that fails to meet customer needs after an attack will likely lose these customers in the aftermath of the attack.

3. A significant attack or disaster can, physically or financially, wipe out a company — and with it all shareholder value. For example, according to USA Today, one year after the 9-11 attacks the rate of bankruptcies in Manhattan had doubled.**

*Australian Institute of Criminology, No. 214, The Detection and Prevention of Cargo Theft, Sept. 2001.

government “bureaucrats” who may lack industry knowledge and experience.

Market-based measures offer greater flexibility, allowing regulated entities to achieve underlying societal goals at the lowest possible expense. In this way, market-based measures can actually drive innovation as companies constantly seek to meet mandates at the lowest possible cost—or better yet with a positive return on investment. They are “enforced” by market competition, providing a constant, ongoing incentive to improve performance and can be easier and quicker to put in place.

These advantages notwithstanding, market-based measures have their own limitations. Many who view the market as an ends will, in knee-jerk fashion, reject any tinkering with the market. Markets would require constant feedback, oversight and management to ensure that they serve the ends desired. Thus far, the information flow between the federal government and private sector has been poor. There is always the potential that a company will decide to simply forego a market-based incentive or suffer a market-based disincentive and not change its behavior. Thus, the market’s day-to-day security incentives and disincentives will likely need to be augmented if the market is to become a force for improved homeland security. That said, in general, market-based measures are strong, flexible, efficient behavioral drivers.

Market-Based Measures for Strengthening Homeland Security

Homeland security market-based measures could take a wide variety of forms. There is, however, one readily available market-based measure that could be quickly and easily used to improve homeland security within most critical infrastructure companies: required disclosures under the existing Securities laws. The application of disclosure requirements here would not require an act of Congress and could be done with little or no new federal dollars.

Disclosure as a market-based measure for homeland security would serve a number of important purposes. First, shareholders are entitled to information concerning all material aspects of those

“They shook America’s throne and struck at the U.S. economy in the heart, thanks to God the Almighty.... Those blessed attacks, as they themselves admitted, have inflicted on the New York and other markets more than a trillion dollars in losses.”

Osama bin Laden, Dec. 27, 2001

companies in which they have investments. Second, requiring disclosure would compel companies to treat homeland security matters not as non-revenue producing costs, but core corporate matters.¹¹ Third, the internal corporate development of appropriate and accurate disclosures will compel senior management to be more directly involved in the security of their companies. Fourth, inadequate disclosures, or the failure to disclose a material issue, can trigger shareholder lawsuits. Such lawsuits—or, as in most cases, the mere threat of such lawsuits—serve as a *de facto* private enforcement program.

The Securities Act of 1933 (1933 Act), and the Securities Exchange Act of 1934 (1934 Act) establish the legal basis for the corporate disclosure requirements enforced by the Securities and Exchange Commission, or SEC. The purposes of the Acts are to protect investors and ensure the fair and efficient functioning of securities markets. Taken together the Acts establish a disclosure-based regulatory scheme requiring dissemination of certain financial and non-financial information in statements filed with the SEC and provided publicly. These rules govern the required annual, quarterly, and other periodic reports.

In general, the securities laws only require disclosure of information that is “material.” Information is “material” if the information is important in influencing a reasonable investor’s investment decisions with respect to a particular company. Since 1982, disclosure under the federal securities laws has been guided by one comprehensive set of regulatory guidelines, Regulation S-K.¹² Three sections of Regulation S-K are particularly germane to the disclosure of homeland security liabilities and concerns.¹³

Item 101 of Regulation S-K (Description of Business)

Item 101 requires companies to provide a host of disclosures, including: the “general development” of their business; the profit or loss and total assets of each segment of its business; the business done and intended to be done by the company and its subsidiaries; and certain information about the geographic areas the company does business. In addition, companies must disclose the material effects on capital expenditures, earnings and competitive position involved with complying, or failing to comply with, federal, state, and local laws.¹⁴

Item 103 of Regulation S-K (Legal Proceedings)

Item 103 requires disclosure of “any material pending legal proceedings, other than ordinary routine litigation incidental to the business, to which the registrant or any of its subsidiaries is a party or of which any of their property is subject.”¹⁵

Item 303 of Regulation S-K (MD&A)

Item 303 requires companies to provide in a clear narrative form a historical and prospective summary of the opportunities and risks impacting the company's results and financial condition.¹⁶ The Management Discussion and Analysis, or MD&A, disclosure "is intended to give the investor an opportunity to look at the company through the eyes of management by providing both a short and a long-term analysis of the business of the company."¹⁷

While Item 303 applies broadly to a company's operations, two areas of disclosure are of particular importance to this analysis: changes to operation and trends and uncertainties. Item 303 requires a narrative disclosure of material changes to a company's operations that could impact profitability and competitive position; specific disclosure of any potential liabilities that may occur because of a company's foreign operations or presence; and provide a forward-looking analysis of perceived trends and uncertainties.

In Securities Act Release 33-6835, the SEC provided guidance as to when a company must disclose a known trend, event or contingency. This guidance provides the following two-prong inquiry as to when to disclose.

1. Likelihood: Is the perceived trend, event or contingency reasonably likely to occur? If management determines that it is not reasonably likely to occur, disclosure is not required.
2. Materiality: If management determines the forward-looking concern is likely, or if it finds it cannot come to a conclusion on likelihood, then the company must objectively decide if the trend, event or contingency will have a material effect on the registrant's financial conditions or operating results.¹⁸

The SEC has recently warned companies that current MD&A analyses are, in general, inadequate. To help companies improve these disclosures, the SEC has raised a series of "hot button" issues that it will be looking at in reviewing future MD&A disclosures. These hot button issues include:

- uncertainty with respect to suppliers;
- planned capital expenditures and related financing (e.g., capital requirements to maintain a growth trend if discontinuation of the trend would be materially adverse);
- uncertainty created by recent legislation;
- impairment of goodwill and uncertainties affecting its recoverability;
- the potential impact of government investigations on expenditures, earnings or competitive position within the industry; and
- insurance issues.¹⁹

“In a matter of time, you will see attacks on the stock market The third letter from bin Laden was clearly addressing using technology in order to destroy the economy of the capitalist states.”

Sheikh Omar Bakri Mohammed (radical Islamic cleric)

Application of Disclosure Requirements to Homeland Security

On their face, these rules would seem to require large amounts of homeland security information be disclosed if this information reaches the materiality threshold with respect to specific companies.

Additionally, a number of factors should be driving companies towards greater—not less—homeland security disclosures including:

- Increasing understanding of the threats to our critical infrastructure, the growing impact of homeland security regulations;
- Growing potential for new homeland security regulation—in particular if the corporate complacency trend continues; and
- Growing combined business impact of all these factors.

While we should be seeing a growing number of homeland security disclosures to shareholders, and a number of companies recognize this requirement, they are the exception and not the rule. And even where such disclosures are made, they are generally not complete.

It is important to underscore that disclosures would not assist terrorists. The types of disclosures discussed above would not provide terrorists with specific operational information about specific targets. In short, SEC-required security disclosures should be strategic and financial, not tactical and proprietary.

In fact, full disclosure by companies that have best-in-breed security programs may actually dissuade terrorist attacks against their facilities. As a general rule, the softer the target the greater the terrorist appeal. If a company’s security systems are the best available, and it says so publicly, it may make itself a far less attractive target.

As a rule, basic threat information, particularly that which is already in the public domain, should be disclosed; classified threat information provided through secure channels should not. The legal right of investors and the market to be informed does not trump the protection of classified and sensitive information.

A market-based SEC disclosure regime should drive internal corporate processes to a higher level and create a regulatory and legal landscape with strong incentives for fuller disclosure.

Current Practice

This section examines the nature and quality of current homeland security disclosures by over forty companies across more than fourteen sectors of the economy that face significant security threats or potential impacts from a terrorist attack.

Homeland Security Sector

The most common form of homeland security disclosure now being made by public companies is information concerning perceived new market opportunities in the homeland security field. For example, the SEC filings of **GSE Systems** (AMEX: GVP), an industry leader in simulations and simulation technology, include a number of discussions about trends in emergency management that open new opportunities for the company.²⁰ Similarly, the **Lockheed Martin Corporation** 2004 (NYSE: LMT) 10-K's MD&A discussion emphasized the potential for increased demand for existing company capabilities.²¹ **CAI International Incorporated** (NYSE: CAI) reflected on increased spending for national defense, intelligence and homeland security.²²

Iconic Companies

Terrorists often select their targets for their symbolic or iconic value. For example, the 9-11 terrorists targeted the World Trade Center because they believed it was a symbol of America's capitalistic system and the U.S. presence in the world. Certain companies are uniquely identified with the American way of life.

According to Paul R. Pillar, a retired CIA officer who was deputy chief of the DCI Counterterrorist Center, "U.S. commercial activity is seen as the leading edge of the American economic and cultural dominance that the terrorists hate so much."²³

Around the world perhaps no company more embodies American culture than the **Walt Disney Company** (NYSE: DIS). The company owns American icons ranging from Disney theme parks and cruise line to the ABC broadcast network. The terrorist threat to the iconic Disney Corporation is significant enough that the Department of Homeland Security has designated the skies over the company's theme parks "no fly zones."²⁴ Despite the seriousness with which the Walt Disney Company takes its security and the terrorist threat to its operations, the company's 2004 10-K makes no mention of terrorism or the terrorist threat.²⁵

McDonald's Corporation (NYSE: MCD) is another inherently American company.²⁶ Overseas McDonald's has suffered a rash of attacks since 9-11 by Islamic terrorists, including Al Qaeda.²⁷ However, the only brief mention of the terrorist threat to the company in its 2004 10-K occurs in a laundry list of risks that might impact performance, which also includes consumer perceptions about the safety of beef and chicken, consumer sending patterns, and potential changes in rules on child-directed advertising.²⁸

In 2000, software giant **Microsoft Corporation** (NASDAQ: MFST), which embodies next-generation American economic and technological thinking and might, became the strongest American brand.²⁹ The

majority of the world's desktop computers run on the company's "Windows" operating system software. Software attacks make up a significant and growing percentage of all cyber-attacks,³⁰ causing widespread disruptions and costly losses.³¹ A 2004 analysis of the global direct costs of a worst-case scenario cyber-worm attack targeting the Windows operating system put the total damages at \$50 billion.³²

Generally speaking, Microsoft's SEC disclosures inform investors that terrorism may impact the market for its goods and services.³³ The company notes that a terrorist attack could materially disrupt its own operations and that cyber attacks are likely to continue.³⁴ In that sense, Microsoft's disclosure is one of the best examples now provided to investors. Its discussion underscores the specific threat to the company; what impact attacks could have; and what the company is doing to protect itself and its investors.³⁵ At the same time, in light of the billions in damages caused by cyber-attacks to date, they seem to materially understate potential risks. For example, these statements do not even allude to the potential for cascading failures of systems control and data acquisition networks, or widespread business disruptions, the type of attack that intelligence suggests terrorists seek to perpetrate.

Most Americans would be highly unlikely to associate coffee giant **Starbucks Corporation** (NASDAQ: SBUX) with terrorism.³⁶ But Internet websites now proclaim that Starbucks is anti-Palestinian/Muslim and pro-Israeli.³⁷ Despite the coffee giant's extensive efforts to address social causes, the company has also become a target for anarchists and others on the radical left. During the 1999 Seattle globalization protests Starbucks was one of the companies vandalized.³⁸

Starbucks' 2005 10-K, however, makes only the most general mention that the company's performance could be affected by a range of factors, including dairy prices, currency fluctuations, and terrorism, among others.³⁹ While, an isolated terrorist bombing on a lone Starbucks' store is unlikely to have a material impact on this sizeable corporation. That said, a string of terrorist bombings at their stores, or for that matter in malls or other places where people gather could significantly impact the company's performance. Additionally, the company does not detail whether and how Starbucks is complying with the security requirements of the 2002 Bioterrorism Act, which includes provisions applicable to food sellers like Starbucks, or other applicable federal security standards.⁴⁰

Wal-Mart Stores (NYSE: WMT), the largest corporation in the world, had \$285.2 billion in sales in the fiscal year ending Jan. 31, 2005.⁴¹ For better and worse, the company has also come to symbolize for many around the world American business and capitalism. The retail giant has suffered a number of bomb scares in its stores across the nation. A pipe bomb was found in the toy department of a Wisconsin Wal-Mart, an improvised explosive device was found in a Wal-Mart in Ithaca, New York., and Molotov cocktails were spread around a Wal-Mart in Philadelphia.⁴²

Wal-Mart's 2005 10-K does not directly address the potential impacts of terrorism on the company's operations. The 10-K obliquely notes that there are risks associated with the significant number of their products being obtained from companies located overseas.⁴³ The 10-K also notes that the company's operations abroad could be impacted by "conditions, economic conditions, legal and regulatory constraints, currency regulations and other matters . . ."⁴⁴ Neither Wal-Mart's 2005 10-K, nor its corresponding Annual Report, address the threats to the company from terrorism at home or abroad in a considered fashion. There is no mention of the attacks on the company's stores. Additionally, Wal-Mart does not address the company's compliance with applicable homeland security laws, regulations and guidance, and the impact of these provisions the company's operations, such as the Bioterrorism Act.⁴⁵

Airlines

The sector most impacted by the 9-11 attacks was, and remains, commercial airlines. The 9-11 attacks were perpetrated using commercial airliners as weapons. Immediately following these attacks the industry suffered serious losses. Congress swiftly acted to federalize security at the nation's airports and impose heightened security requirements on the carriers. For these reasons, it is not surprising that homeland security disclosures are common across this sector.

United Airlines' (NYSE: UAL) 2004 Report provides an extensive review of the implications of the Aviation and Transportation Security Act, enacted in November 2001, which included the imposition of a passenger security fee.⁴⁶ It also discussed the legal actions the company faces as a result of the 9-11 attacks and the potential relief offered through the victim compensation fund established under the legislation.⁴⁷ Interestingly, American Airlines, the other airline directly attacked on 9-11, did not discuss these legal actions.

The airlines as a group also all similarly discussed the impact of terrorism insurance on their operations. For example, **Delta Airlines'** (NYSE: DAL) 2004 Form 10-K highlighted the importance of government support on insurance availability and the added expense and uncertainty, including potential interruption of operations, if that support ended.⁴⁸ Delta's 2004 annual report also provided a substantial, forward-looking discussion of the airline's security program, including expanding partnerships with other homeland security players and the use of technology for access controls and information sharing.⁴⁹ However, the company's 2004 Form 10-K does not provide similar insights to investors.

Southwest Airlines' (NYSE: LUV) 2004 Report was the only one to discuss, albeit briefly, how heightened security is impacting the "airport experience for passengers."⁵⁰ Southwest went on to discuss how it was making substantial investments to process passengers efficiently and "restore the airport experience" for its fliers.⁵¹ Southwest's 2004 Annual Report discusses this effort at some length, including efforts to speed check-in procedures and improve baggage screening.⁵²

Apart from potential 9-11 liabilities, every one of these airlines faces essentially the same on-going threats and security requirements. Yet, apart from fairly uniform insurance disclosures, there are substantial differences between and among their disclosures of security concerns. Each of these approaches has merit. They all disclose information that the reasonable investor would want to know in order to make informed investment decisions. However, no disclosure touched on all these bases.

Chemicals

If the airline industry has faced the greatest impacts of homeland security to date, the chemical industry is, arguably, the industry most likely to next face considerable regulation.

A number of recent news reports raise serious concerns about vulnerabilities in the chemical sector.

In 2004, Robert Full, Chief of the Allegheny County Department of Emergency Services in Pennsylvania told a House subcommittee that, with regard to some of the nation's most dangerous chemical plants in his area, "Some of the facilities have no more security than maybe perhaps a

padlock or a chain.”⁵³ According to the Environmental Protection Agency, at least 123 plants reported a worst-case scenario with a vulnerability zone containing more than a million people.⁵⁴

According to the Global Security News, of 15,000 chemical plants in the U.S. that produce, use or store at least one of the 140 toxic and flammable chemicals that the EPA designates as potentially harmful to humans, only 2,200 of these plants are subject to the federal terrorism security requirements of either the Public Health Security and Bioterrorism Response Act of 2002 or the Maritime Transportation Security Act of 2002. An additional 1,100 are required through their membership in the American Chemistry Council (ACC) to conduct vulnerability assessments and adopt a voluntary “security code.”⁵⁵

In other words, security at the vast majority of these plants is subject to neither mandatory nor voluntary baselines. Secretary of Homeland Security Michael Chertoff favors the creation of a regulatory framework.⁵⁶ Congress is considering legislation.⁵⁷ New chemical security mandates may require many facilities to invest significant amounts of money on security upgrades, be subject to enforcement provisions, litigation and penalties, or, perhaps even, require inherently safer production processes.

Despite these changes and uncertainties, the SEC filings of the nation’s chemical companies offer virtually no sense of the evolving impacts of security on the competitive marketplace. A review of the public companies that operate plants that have been identified as among the nation’s deadly facilities⁵⁸ found that only three of these companies even alluded to the risk of terrorism, albeit in oblique ways.⁵⁹

The 2004 Form 10-K of the **E. I. du de Nemours and Company** (NYSE: DD), better known as DuPont, stated that “[T]he company’s business and profitability in a particular country could be affected by political or economic repercussions on a domestic, country specific or global level from acts of terrorism or war (whether or not declared) and the response to such activities.”⁶⁰

The **Ferro Corporation’s** (NYSE: FOE) 2004 Form 10-K listed “terrorism” in a chart of potential risk factors.⁶¹ The **Occidental Petroleum Corporation’s** (NYSE: OXY) 2004 Form 10-K briefly noted that the company does business in countries where there is the risk of “armed conflicts” and “security problems.”⁶²

None of these filings discussed the potential impact that a new homeland security regulatory regime could have on corporate operations, capital expenditures, legal proceedings, or other areas of business. Apart from the mere mentions by these three companies, none of the other companies even noted the potential terrorist risks to their operations—even though an attack on any of these facilities could potentially impose immense liabilities on the company—nor actions taken in response. In short, all these filings arguably failed to disclose homeland security information that was obviously material to the reasonable investor.

Freight Rail

Another sector that is now the focus of extensive homeland security concerns is the freight rail industry. Heightened concerns of terrorist threats to rail systems, following the recent London and Madrid attacks, have brought considerable attention to rail security, particularly hazardous materials shipped by rail through target cities including the nation’s Capitol. Senator Joseph Biden, who has proposed wide-reaching rail cargo security legislation, has repeatedly highlighted the danger:

[T]he Naval Research Laboratory has estimated that up to 100,000 people could be killed or injured in less than a half-hour by such an attack.⁶³

In response to these concerns, the District of Columbia's City Council enacted a ban on shipments of hazardous materials, including by rail, through the District. On appeal from the lower court, the District of Columbia Court of Appeals enjoined the ban and sent the matter back to the trial court. While the case is still under consideration, a number of other cities are moving ahead with their own rail security measures, including bans on shipments through certain corridors.⁶⁴

The potential for a series of local security requirements covering key rail corridors, creating a crazy quilt of differing—if not conflicting—security requirements and or bans is of significant concern to the railroads. Re-routing options are limited. Even a handful of local actions could significantly affect a freight carrier's operations.

In its 2004 Form 10-K, **CSX Corporation** (NYSE: CSX), the railroad that operates the contentious route through Washington, D.C., provided the following disclosure:

Certain metropolitan areas considered a security risk have been and may continue to be the subjects of regulation. The ultimate legislation passed by federal, state and local regulators related to issues of security has the potential to materially adversely affect CSX's operations and costs.⁶⁵

CSX also noted the overall risk of terrorism to its operations.⁶⁶ Interestingly, in response to these concerns, CSX has undertaken substantial security efforts within the Washington, D.C. corridor. However, the company did not discuss its efforts to counter the threat of terrorism.

Union Pacific Corporation's (NYSE: UNP) 2004 Form 10-K acknowledged that it could be a terrorism target, which would affect its operations, financial condition, liquidity and insurance coverage.⁶⁷ However, Union Pacific's 2004 Report made no mention of the adequacy of the railroad's security efforts to address this threat. Union Pacific operations encompass a number of areas that are of significant concern for terrorist attacks against railroad operations, such as Los Angeles, Houston, Chicago, Portland, Seattle, Dallas and Phoenix.

Kansas City Southern's (NYSE: KSU) 2004 10-K noted that the government response to terrorism could also materially impact the company's operations. The company, unlike the other railroads, also mentioned the potential impact of terrorism risk insurance costs on the railroad's profitability.⁶⁸ By contrast, **Burlington Northern Santa Fe Corporation** (BNSF) (NYSE: BNI) only named terrorism in a laundry list of potential operating problems, which also included severe weather and earthquakes.⁶⁹ BNSF made no mention of the risk to rail operations, even though BNSF's areas of operation includes Chicago, Houston and San Francisco, all vital transportation hubs within striking distance of major population centers and likely terrorist targets.

The Norfolk Southern Corporation's (NYSE: NSC) 2004 10-K makes no mention of the terrorist threat to the railroad's operation.⁷⁰ Nor does the 2004 10-K discuss the potential impact of new security mandates on the company rail security legislation. This omission occurs despite the fact that Norfolk Southern operates in a number of areas at a heightened risk to terrorism, including the highly populated corridor running from the New York-New Jersey area, through Baltimore and Philadelphia, down to

Washington, DC. The company's rail lines also serve important military bases and operations in and around Norfolk, VA.

Canadian Pacific Railway's (CPR) (NYSE: CP) 2004 Form 10-K took a different approach, focusing on the impact of border security on the company and giving extensive detail of security actions taken, including participation in government-sponsored programs, and their cost:

The Government of Canada and CPR have each committed up to \$4.1 million to secure the rail corridor between the Windsor VACIS facility and the U.S. border. This joint government-industry initiative is expected to enhance the security of U.S.-bound rail shipments while helping to ensure uninterrupted access to the U.S. market for CPR customers.⁷¹

CPR raises the sort of homeland security information investors have the right to know. CPR's discussion here should be contrasted with the lack of discussion from other companies, such as large-scale retailers, that could similarly be impacted by terrorism impact on trade flows. What is unsaid is the potential impact should a terrorist attack close the border between the U.S. and Canada for any period of time, which could seriously harm the railroad.

Hospitals

America's hospitals and healthcare system are vital to preparing this nation for any terrorist attack. At the same time, our hospitals have little excess or surge capacity, face significant cost-cutting pressures and have received little federal assistance in preparing for their role in this fight.

A mass casualty event, in particular a WMD terrorist attack, on the United States will have a major impact on the nation's healthcare system. Affected hospitals will be overwhelmed. The business of healthcare at these facilities will cease. In addition, depending on the nature of the attack, there is the potential that affected hospitals may find themselves contaminated and shuttered.⁷² In addition, if these hospitals cannot provide adequate protection for their staffs and patients they may face both high workers compensation claims and negligence lawsuits.⁷³

A GAO study examined the bioterror response preparedness of 2,041 urban hospitals—the healthcare facilities that will most likely bear the brunt of a terrorist attack against the United States. According to the GAO, “Hospital officials have told us that bioterrorism preparedness is expensive and they are reluctant to create capacity that is not needed on a routine basis and may never be needed at a particular facility.”⁷⁴ In other words, the vast majority of the nation's urban hospitals are unprepared to handle a bioterrorism attack.

At the close of 2004, **Hospital Corporation of America** (NYSE: HCA) owned and operated 174 general, acute care hospitals, and an additional six through joint ventures, across 23 states.⁷⁵ HCA's 2005 10-K discusses a host of legal and regulatory issues, as well as societal shifts that could impact the company. However, the 2005 10-K only mentions the terrorist threat once as part of a laundry list of things that could impact the company's performance.

Tenet Healthcare Corporation (NYSE: THC) is the nation's second largest investor-owned health care services company in the United States. At the close of 2004, THC operated 80 general hospitals

(two of which were classified as critical access hospitals) in thirteen states.⁷⁶ The company is increasingly shifting its operations to focus on the nation's metropolitan areas, such as Philadelphia, Los Angeles, Miami and Houston.⁷⁷ While the company's 2005 10-K provides extensive and informative discussions of a host of factors impacting Tenet's operations, it makes no mention of the risks from terrorism.

Real Estate Investment Trusts

Real Estate Investment Trusts, "REIT's," own vast amounts of property across the nation, ranging from skyscrapers in major cities, to malls, to luxury hotels. In many instances, this real estate is located in areas that are at substantial risk to terrorism. The value of these properties as investments can be adversely impacted if a terrorist attack simply occurs around them, perhaps in their neighborhood—let alone against them directly. A nuclear or radiological attack could render them permanently or temporarily uninhabitable.

One of the most important security impacts on the REIT business climate is in the area of insurance. The attacks of 9-11 resulted in an estimated \$32.5 billion in insured losses, the most costly catastrophe ever.⁷⁸ The impact on insurance markets was extreme.⁷⁹ Many companies in high risk areas could no longer obtain comprehensive risk insurance (including terrorism) at any price.⁸⁰ Where companies could still obtain insurance, the cost of insurance was high.⁸¹ Some companies were forced to operate without coverage or with grossly inadequate coverage.⁸² In a number of instances lenders sought to enforce loan terms requiring comprehensive terrorism coverage.⁸³ One such case involved the Mall of America, with the lender going to court to seek repayment for breach of contract.⁸⁴ Major development projects fell through because terrorism insurance could not be obtained.⁸⁵

Eventually, Congress passed and the President signed TRIA in November of 2002, with a December 31, 2005 (since extended to 2007) sunset provision. From a disclosure perspective, the uncertainty around TRIA's future in 2005 would seem to be a material fact for REIT's that should have appeared in corporate filings prior to the extension. Additionally, from a forward-looking perspective, TRIA's uncertain future beyond 2007 is likely a material matter. Likewise, changes in building codes and design in light of the threat of terrorism, including improved fire resistance and egress standards, could materially impact certain REITs.⁸⁶ Unfortunately, REIT disclosures to date are also generally inadequate.

The **Simon Property Group** (NYSE: SPG) owns close to 300 income-producing properties mostly in and around major metropolitan areas, such as New York City, Los Angeles, Chicago, Boston, Washington, D.C., San Francisco, and Atlanta, and tourist destinations, such as Orlando and Las Vegas. Until 2003 Simon was the majority owner and operator of the Mall of America, believed by DHS and others to be a potential terrorist target.⁸⁷ Yet the 2003 Form 10-K made only a brief reference to the impact of "[t]he events of September 11, 2001" on the company's insurance program.⁸⁸ Even this mention did not fully capture the fact that the company was sued by its lender for the failure to have terrorism risk insurance.⁸⁹

Ramco-Gershenson Properties Trust (RGPT) (NYSE: RPT) is a somewhat similarly situated, publicly-traded REIT. The only mention of terrorism in its 2005 Form 10-K appears in a condition to a promissory note provided as an attachment to the annual report.⁹⁰ RGPT's 2005 10-K did not mention

TRIA issues. The SEC filings of the **Heritage Property Investment Trust** (NYSE: HTG), whose holdings include three office buildings in New York City, does state, “If one of these [catastrophic] events occurred to, or caused the destruction of, one or more of our properties, we could lose both our invested capital and anticipated profits from that property.”⁹¹

Contrast these examples with that of **Boston Properties** (NYSE: BXP), one of the nation’s largest owners, managers, and developers of office properties. Boston Properties 2005 10-K clearly underscores the terrorism risk to the company:

We have significant investments in large metropolitan markets that have been or may be in the future the targets of actual or threatened terrorism attacks, including midtown Manhattan, Washington, D.C., Boston and San Francisco. As a result, some tenants in these markets may choose to relocate their businesses to other markets or to lower-profile office buildings within these markets that may be perceived to be less likely targets of future terrorist activity. This could result in an overall decrease in the demand for office space in these markets generally or in our properties in particular, which could increase vacancies in our properties or necessitate that we lease our properties on less favorable terms or both. In addition, future terrorist attacks in these markets could directly or indirectly damage our properties, both physically and financially, or cause losses that materially exceed our insurance coverage. As a result of the foregoing, our ability to generate revenues and the value of our properties could decline materially. See also “—*Some potential losses are not covered by insurance.*”⁹²

The company also discusses in great detail the terrorism insurance issues it faces, along with the rest of the sector and steps the company has undertaken to address these issues.⁹³

From an investor’s standpoint this information is among the best homeland security disclosures of all publicly traded companies.

Equity Office Properties Trust (NYSE: EOP) also provides a fuller discussion of the potential impact of terrorism on its operations. Equity is the nation’s largest publicly held owner and manager of office properties, with buildings located in the heart of Washington, DC, Manhattan and Chicago. Equity’s 2005 filings incorporate by reference the risk discussions from the company’s March 2004 8K, which stated that as a result of a terrorist attack, “the market value of our securities could decline.”⁹⁴ Equity’s 2005 10-K also discusses the importance of TRIA to its business and the uncertainty over its extension.⁹⁵ While Equity is clear about the terrorism risks to its operations, it does not discuss what steps the company may have taken to address or mitigate these risks.

Few companies understand the direct impacts of terrorism better than the **Host Marriot Corporation** (NYSE: HMT). Its New York Marriot Financial Center hotel was damaged in the 9-11 attacks and required extensive repairs. The company’s 2005 10-K provides one of the most extensive discussions of the terrorism insurance issues facing countless companies:

Some potential losses are not covered by insurance... there are other risks such as war, certain forms of terrorism such as nuclear, biological or chemical terrorism and some environmental hazards that may be deemed to fall completely outside the general coverage limits of our policies or may be uninsurable or may be too

expensive to justify insuring against. If any such risk were to materialize and materially adversely affect one or more of our properties, we would likely not be able to recover our losses.⁹⁶

However, the company does not address the terrorism risk to its properties, nor the likely economic ripple effect on business travel and tourism if there is another attack. Finally, apart from insurance, Host Marriot does not mention any steps taken to diminish the risk of terrorism to its operations, employees, customers, properties, and, in turn, investors. Here the company arguably does itself a disservice.

Starwood Hotels and Resorts Worldwide's (NYSE: HOT) focuses on hotel and leisure properties. Starwood's 2005 10-K included a broad-form disclosure that terrorism, war and other forces majeure could have a material impact on its operations and anticipated results, including insurance limits.⁹⁷ But the company does not offer its investors a forward-looking discussion as to the potential wider impacts of terrorism on results. Its 10-K offers no information about what steps, apart from insuring against this risk, the company has undertaken to secure itself.

The REIT industry also plays an important role in America's industrial economy. For example, **First Industrial Realty Trust, Inc.** (NYSE: FR) is the nation's largest provider of diversified industrial real estate. First Industrial's holdings are the types of facilities that other companies' supply chains are dependent upon—manufacturing, light industrial, regional warehouse and bulk warehouse. Supply chains that run through transportation hubs in Northern New Jersey, Philadelphia, Houston and Los Angeles raise major homeland security concerns. An attack, especially a WMD attack, at one of these ports could cause major human and economic damage. However, the company's 2005 10-K does not address the threat of terrorism to supply chain properties in these particular markets. Further, the 2005 10-K does not address who is responsible for security at the company's leased properties. No mention is made of what role security plays in determining to whom First Industrial will lease its properties.

Nuclear Energy

Within the energy sector, perhaps the greatest security concerns focus on the nation's nuclear power plants. An attack against one of these plants could have devastating consequences, including hundreds of thousands of casualties and the risk of immense contamination. Security at these facilities has been plagued by serious problems.⁹⁸ For example, these companies failed just under 50 percent of the mock terrorist attacks conducted by the Department of Energy⁹⁹—even though facilities were given advance notice of the tests.¹⁰⁰

Entergy Corporation (NYSE: ETR) operates five nuclear plants in New York, Massachusetts, Vermont, Arkansas, Louisiana, and Mississippi. Of particular concern is the company's Indian Point plant located in Buchanan, New York, just 35 miles north of midtown Manhattan. Roughly 300,000 people live within ten miles of this plant alone. A 2002 study of security at Indian Point by an outside consultant to Entergy found that 81 percent of the facility's own guard force believed they could not adequately defend the nuclear plant.¹⁰¹ While the Federal Emergency Management Agency has certified the facility's evacuation plan, an independent report commissioned by New York Governor Pataki by James Lee Witt, the Director of FEMA under President Clinton, determined that the Indian Point evacuation plan was flawed and inadequate.¹⁰² The federal government's worst case scenario estimate for a failure or attack on this plant are 221,000 casualties and up to \$314 billion.¹⁰³

Energy's 2004 10-K mentions terrorism in an extensive list of risks that could impact the company's performance.¹⁰⁴ It also mentions the federally mandated insurance program that the company and other nuclear plants operate under.¹⁰⁵ It does not address the potential liabilities the company might face in the event of a terrorist attack at its Indian Point Plant or its other nuclear facilities, nor its security performance.¹⁰⁶

Exelon Corporation (NYSE: EXC), the nation's largest nuclear operator, operates the Limerick nuclear power generating plant, about 40 miles northwest of Philadelphia. The Limerick facility is old and its design puts the facility at heightened risk to certain types of terrorist attacks. Exelon's 2005 Form 10-K generally raises the issue of the terrorist threat to the energy industry:

Exelon has initiated security measures to safeguard its employees and critical operations from threats of terrorism and is actively participating in industry initiatives to identify methods to maintain the reliability of Exelon's energy production and delivery systems. Additionally, the energy industry is working with governmental authorities to ensure that emergency plans are in place and critical infrastructure vulnerabilities are addressed in order to maintain the reliability of the country's energy systems. These measures will involve additional expenses to develop and implement, but will provide increased assurances as to Exelon's ability to maintain critical operations.¹⁰⁷

The 10-K also separately underscores the company's compliance with security requirements for nuclear power facilities.¹⁰⁸ It does not address in any substantive way the specific threats to Exelon specifically, such as the proximity of the Limerick plant to Philadelphia.

Transborder Supply Chain

Vast numbers of American companies are increasingly reliant upon global supply chains to deliver everything from raw materials to finished products to their operations and customers. Each year more than sixteen million ocean-going loaded marine containers enter the United States offloaded from thousands of container ships.¹⁰⁹

The fast and efficient movement of goods and materials through supply chains are vital to the U.S. economy. If these just-in-time supply chains are interrupted, the impact would be significant. A 2002 simulation of a container cargo attack determined that such an attack would close every American port, resulting in \$58 billion in losses to the American economy.¹¹⁰ Similarly, U.S. Coast Guard officials believe that the closure of a single major port for just one month because of a terrorist attack could cost the United States \$60 billion in economic losses.¹¹¹ Yet, Stephen Flynn, a retired Coast Guard officer expert in cargo security, has determined that, under the best circumstances, existing targeting and inspection programs have less than a 10 percent chance of detecting a nuclear weapon concealed in containerized cargo being shipped to the United States.¹¹²

The federal government has taken a number of steps to improve cargo, supply chain and port security, including the Customs-Trade Partnership Against Terrorism (C-TPAT) and Container Security Initiative (CSI). The post-9-11 MTSA imposes a series of security requirements on the physical port operations and maritime vessels.¹¹³ Facilities that are not in compliance with the rules can be fined or closed.¹¹⁴ If the Coast Guard determines security at a foreign port is inadequate, vessels making port calls at

that port may be denied entry into U.S. waters.¹¹⁵ Many experts and legislators believe that additional supply chain security measures are still necessary, which could impact every company with global supply chains.¹¹⁶

Eighty percent of Wal-Mart's suppliers are located in China, making it the single largest importer of foreign goods to the United States and highly dependent upon a vast, global supply chain.¹¹⁷ Yet Wal-Mart's 2005 10-K does not address the importance of an unbroken, delay-free supply chain to its business, nor how fragile it may be to a terrorist attack. Ironically, the company does not address any of its industry-leading security efforts, which include requiring its top suppliers to put "Radio Frequency Identification" (RFID) tags on all crates and pallets. Moreover, to avoid disruptions—ranging from congestion delays to terrorism—Wal-Mart ships products through nine major ports.¹¹⁸ However, because of Wal-Mart's failure to disclose these security programs, the company's investors and potential investors have no knowledge of this comparative advantage.

Similarly, **Target's** (NYSE: TGT) business model and bottom-line are highly dependent on the unfettered movement of products along a far-reaching supply chain. Target is the second largest importer of containerized cargo.¹¹⁹ Target management played a key role in the development of the C-TPAT program and the company was one of the seven charter members in the program.¹²⁰ Target's 2005 Form 10-K makes just one passing reference to the potential terrorism impact on the company's performance.¹²¹ The company's 10-K makes no direct mention of the threat to Target's supply chain. The 10-K does not discuss Target's participation in either C-TPAT or Operation Safe Commerce,¹²² nor its RFID directive to its shippers.¹²³

Seaspan (NYSE: SSW) is one of the few major containerized maritime shipping companies traded on U.S. markets. The company operates a fleet of thirteen containerships. Seaspan issued its first shares on the New York Stock Exchange in 2005 and has not yet filed a form 10-K. However, Seaspan's F-1 provides a relatively extensive discussion of the risk of terrorism to the company and maritime shipping companies generally:

Terrorist attacks targeted at sea vessels, such as the October 2002 attack in Yemen on the VLCC Limburg, a ship not related to us, may in the future also negatively affect our operations and financial condition and directly impact our containerships or our customers.¹²⁴

The company's form F-1 also notes that the company's bottom-line could be materially impacted by terrorism-related business interruptions, higher insurance costs, and loss of revenues and contracts.¹²⁵ In relative terms, Seaspan's initial filing offers investors a significantly better understanding of the risk of terrorism to the company than most other companies provide, although there are also a number of gaps.

The Matson Navigation Company is a subsidiary of **Alexander & Baldwin Inc.** (NASDAQ: ALEX). Matson operates a fleet of seventeen vessels and provides integrated supply-chain logistic services. The only mention of the risks to the company from terrorism in the 2004 10-K of Matson's parent company occurs as a passing reference in a laundry list of general risks, such as litigation and performance of pension assets.¹²⁶

In contrast, Canadian maritime shipping company **CP Ships** (TO: TEU.TO), traded on the Toronto exchange, has a fleet of 79 ships that run on 23 trade lanes focusing on TransAtlantic, Australasia,

Latin America and Asia shipping, making it the sixteenth largest carrier in the world.¹²⁷ CP Ships' 2004 Annual Information Form discusses the issue of supply chain security; the requirements of new U.S. maritime security legal requirements; Canadian security regulations under which it now operates; and how supply chain security requirements may impact the company's performance.¹²⁸ CP Ships also provides a brief mention that the company could suffer uninsured losses in the event of a terrorist attack.¹²⁹ CP Ships disclosures provide investors a fairly full understanding of the impact of homeland security and terrorist activity on the company, though not the sector more broadly.

United Parcel Service (NYSE: UPS) is the world's largest package delivery service.¹³⁰ The company's international package operations include delivery of goods to over 200 countries and territories worldwide.¹³¹ In 2004, the company moved an average of 14.1 million packages per day.¹³² UPS is also increasingly focused on B2B supply chain management services, including customs brokerage assistance.¹³³

The impact of 9-11 on UPS demonstrates how terrorism can materially impact a company. According to UPS, the 9-11 terrorist attacks cost the company approximately \$130 million, which drove down earnings per share.¹³⁴ However, the company does not address the potential of another attack on its business operations. UPS does provide an assessment regarding potential new air cargo security requirements, although it materially downplays the cost of new rules compared to what industry groups have told the Transportation Security Administration.¹³⁵

Insurance

Terrorism presents special challenges to the insurance industry. It is difficult to objectively quantify the overall risk of terrorism to the nation, a region, a city, or an industry—let alone an individual company.¹³⁶ The attacks of 9-11 were the single largest losses ever suffered by the industry. As such, terrorism defies the insurance industry's current actuarial and business models. To date, the industry has yet to develop an effective means of determining the risks to companies seeking policies. This situation creates real competitive challenges for the industry—particularly if TRIA expires at some point. Client companies want and need terrorism insurance policies. In the absence of more defined homeland security regulations, insurers may play a significant role in shaping the security programs of their critical infrastructure clients. As such, terrorism presents real risks and potential advantages to actors in this sector.

American International Group, or AIG (NYSE: AIG), is one of the largest insurance companies in the United States. AIG alone suffered a loss of approximately \$820 million as a result of the 9-11 attacks.¹³⁷ AIG's 2005 10-K includes a brief statement about the company's leadership in efforts to renew TRIA, but no additional information about the impacts if TRIA expired.¹³⁸ The 10-K also makes very brief mention of the risk of terrorist attacks as one of many risk factors to the company's success.¹³⁹

Aon Corporation (NYSE: AOC), another industry leading insurance and reinsurance company, suffered far more than mere economic losses in the 9-11 attacks—the company had offices in the South Tower of the World Trade Center and 176 of its employees were victims of the attacks. Aon's 2004 Annual Report makes no mention of terrorism, TRIA uncertainties or other homeland security matters.¹⁴⁰ The company's 2005 10-K notes only that Aon's performance could fluctuate because of a range of factors including terrorism¹⁴¹, even though a company press release stated that "that the private insurance market cannot operate without some form of public backstop against catastrophic terrorism losses."¹⁴²

Marsh & McLennan (NYSE: MMC) also had offices in the World Trade Centers and lost 295 employees in the attacks. In addition, MMC suffered uninsured pre-tax losses of \$126 million from the 9-11 attacks.¹⁴³ That said, MMC's 2004 Annual Report and Form 10-K make only one brief mention of the risk of terrorism to the company in a laundry list of risk factors.¹⁴⁴ The company does not discuss the uncertainties surrounding TRIA, nor any substantive analysis of terrorism risk and how it could affect MMC.

Analysis

As the examples above show, the current practice of homeland security disclosures under law by public companies is highly inconsistent. Many companies simply do not provide their shareholders with homeland security information that the average investor would likely view as material to their investment decisions. This undermines a basic tenet of the securities laws and markets.¹⁴⁵ Because companies that more fully discuss security risks may be hurt by their disclosures vis-à-vis competitors who take it less seriously, incentives are turned on their head. Markets could punish the most secure companies.

Sarbanes-Oxley and Private Sector Homeland Security

The Sarbanes-Oxley Act ("SOX") may also play an important role in corporate homeland security.¹⁴⁶ Like the 1933 and 1934 Acts, Congress passed SOX in the wake of high-profile scandals.¹⁴⁷ The stated purpose of the act was to ensure greater compliance with financial reporting requirements and implement specific measures to insure the accuracy and transparency of these reporting requirements. Specifically, it requires public companies to adopt, implement, and certify to the existence of internal procedures adequate to identify and properly disclose material changes in financial conditions and results, including expectations of future performance.¹⁴⁸

There is a clear convergence of homeland security interests and the fiduciary responsibility of corporate management.¹⁴⁹ Given the clear link between homeland and economic security, Sarbanes-Oxley should put companies on notice that they should support their homeland security disclosure decisions with an internal procedure for identifying, quantifying and assessing the materiality of these issues.¹⁵⁰ Management needs to be informed about and engaged in corporate homeland security decisions. A failure to properly disclose corporate homeland security matters can result in real consequences for senior management.

The SEC itself has authority to enforce and bring such cases. Therefore, smart companies would be wise to ensure that they have made appropriate homeland security disclosures based on an informed, documented process. While there is no authoritative statement or resource outlining what a SOX homeland security governance process should look like, corporate experience in the environmental area offers a potential model.¹⁵¹ Compliance should include:

- A committee of directors with direct oversight of security related matters;
- Formal board level review or audit of security related matters; and,
- Creation of a chief security officer who reports directly to the CEO or to independent directors.

SEC Options for Strengthening Homeland Security Disclosures

SEC action should provide an incentive for stronger private sector critical infrastructure protection. There are a number of steps the SEC could take to make it clear to all public companies that they are required to fully disclose material homeland security information to their shareholders. Available options include:

- Placing homeland security issues on its list of hot button concerns and using its bully pulpit to inform public companies that the SEC intends to take a closer look at such issues in future corporate filings.
- Reviewing a series of corporate filings and issuing “comment letters” back to the reviewed companies regarding the adequacy of homeland security disclosures. These letters are also released to the public, allowing the agency to send a broad message about what is expected.
- Issuing “interpretive guidance” on the importance of homeland security and how it should be addressed. In 2001, the SEC issued such “Cautionary Advice” that public company disclosures under the MD&A requirements should be enhanced.¹⁵²
- Commencing one or more high profile enforcement actions against regulated companies that have not, in the Commission’s view, made required homeland security disclosures under present rules.

The problem, however, is that homeland security matters do not fit neatly within current concepts of material information that must be disclosed. At present the issue of materiality is driven mainly by the bottom-line: will the feared occurrence have a material impact on corporate performance—read as revenues, earnings per share, and other core economic indicators of company success.¹⁵³ While homeland security matters can clearly impact corporate performance, greater, long-term attention to homeland security is fundamentally an issue of national security.

During the late 1970’s and early 1980’s, the SEC confronted a similar challenge amid growing concern over corporate environmental performance. Shareholders wanted more information as environmental laws and regulations were growing stricter and were beginning to be seriously enforced. This created the potential for serious corporate liabilities. At the same time, environmental groups were making the positive case that sound environmental stewardship was good for corporate performance. Yet, few companies were alerting their shareholders to environmental matters.

In response, the SEC issued three disclosure requirements specific to environmental matters:

- Item 101 of Regulation S-K requires companies to disclose the material effects of compliance with existing environmental laws.¹⁵⁴
- Item 103 of Regulation S-K requires companies to describe “any material pending legal proceedings, other than ordinary routine litigation incidental to the business, to which the registrant or any of its subsidiaries is a party.” This applied to any material administrative or judicial proceedings arising under federal, state, or local environmental laws or regulations; and any environmental enforcement matters that might reasonably be expected to result in

sanctions of \$100,000 or more, even where the proceeding might otherwise be considered immaterial to the company's operations or bottom-line.¹⁵⁵

- Item 303 of Regulation S-K requires companies to disclose “any known trends, demands, commitments, events or uncertainties” that are reasonably likely to have a material effect on a company's bottom line.¹⁵⁶ While the text did not specifically address environmental matters, the SEC's interpretive bulletin used two environmental hypotheticals of required disclosure.¹⁵⁷

These rules have perceived shortcomings. The SEC is now facing increasing heat from environmentalists, members of Congress, corporate watchdogs and even some progressive business experts who believe that companies are not adequately complying with these requirements. Even so, the application of similar requirements in the area of homeland security would represent a quantum leap forward. As such, the environmental rules serve as both precedent and model for homeland security specific disclosure requirements.

That said, any new SEC homeland security requirements or guidance must reflect the specific sorts of homeland security information that would be most valuable to shareholders. Homeland security rules should require disclosure of the following types of information:

- **Threats:** What is the nature of the threat (if any) to the company specifically or its market sector generally?
- **Impacts:** What sorts of impacts would an attack on the company reasonably be expected to produce? What impacts would a worst case scenario result in?
- **Precautions:** What steps has the company undertaken to counter the threats it faces?
- **Market Impact:** To what extent does the company believe homeland security policy changes will have a material impact—positively or negatively—on the market a company competes in?
- **Comparative Advantage and Disadvantage:** Does the company's homeland security efforts provide it with a comparative advantage, or burden it with a comparative disadvantage, over the short- or long-term vis-à-vis competitors?
- **Compliance:** What material effects do voluntary security requirements have whether or not the company chooses to comply? Are emerging homeland security laws reasonably expected to have a material effect on the company's operations or bottom-line? Is the company aware that it is not in full compliance with any homeland security legal requirement? Is the company aware that a governmental agency has begun, or is beginning, a homeland security compliance action?
- **Impending Legal and Regulatory Issues:** Does the company know that it may soon face a new federal, state, or local mandate that would materially impact its operations?
- **Spending:** What level of investment is the company making in its security? What are the trends in the company's security spending?

Finally, any change to the SEC rules to focus on homeland security matters should address the issues of materiality and probability. If the goal is to encourage broader corporate disclosures as a vehicle for better homeland security performance, the SEC will need to provide further guidance as to what constitutes materiality for homeland security purposes. A new standard could eliminate the materiality test (as was done in the case of certain environmental sanctions): if this applies, it must be disclosed, full stop.

Probability here should reflect our growing understanding of modern-day terrorism. Otherwise, because it is impossible to predict with any certainty when and where the terrorists will strike next, companies that do not want to disclose serious homeland security concerns will simply use improbability as a shield against disclosure. While no company has a crystal ball, it can determine within an acceptable margin of error macro-level risk based on sector, geographic presence and other corporate characteristics.¹⁵⁸

To date, the SEC has been silent on how companies should handle disclosure of homeland security matters. Congressman Chris Cox, the new SEC chair and former chairman of the House Committee on Homeland Security, is intimately familiar with the terrorism threat to the United States. He will be in a strong position to incorporate homeland security issues into SEC rules.

Overcoming the Ostrich Problem

The effectiveness of a disclosure-driven, market-based system for enhancing critical infrastructure homeland security is largely dependent upon the quality of information available to each company's leadership—and in turn shareholders and the market. Simply put, “garbage in, garbage out.”

Some companies are already opting not to know. Many companies have not conducted top-to-bottom security assessments, or audits, because they are concerned that such a review will bring to light serious security shortcomings. These companies fear that once they are aware of such shortcomings they will either have to spend vast amounts of money to fix them, or risk serious liabilities for willful negligence if something bad happens to the company. This is the proverbial “Ostrich Problem.”

In fact, the decision not to know, and the resulting ignorance, actually offers companies little protection. There is ample legal precedent that willful blindness is not a shield against liability—in either shareholder derivative actions or liability lawsuits. A market-based, disclosure regime will function best if companies are positively encouraged to analyze and fully understand their risks and the effectiveness of their security systems, and can then communicate such information to the market.

Policymakers previously confronted a very similar dilemma in the environmental compliance and policy area. During the 1980's, many companies were concerned about the liabilities environmental audits might trigger. To correct this problem, all but nine states have adopted so-called Environmental Audit Shield Laws or self-policing enforcement policies that protect and incentivize self-disclosure.¹⁵⁹ While each state's law is unique, at base all of these laws protect a company that on its own undertakes an environmental audit of its operations and then takes reasonable steps to address any shortcomings identified in such an audit.

At the federal level, in 1995, the Clinton administration adopted a new environmental enforcement policy for companies that had undertaken self-audits.¹⁶⁰ The 1995 federal audit enforcement shield

policy, in many cases, completely waived fines and penalties for violations of environmental laws where the company self-disclosed the problem and took adequate steps to address the violation. In 2000 this policy was revised to further increase the incentives for self-auditing, disclosure and improvements.¹⁶¹ A 2004 empirical analysis of state and federal audit shield-type policies determined that such policies resulted in significant environmental gains—they achieved their underlying policy goals.¹⁶²

Federal law already provides a limited information safe-harbor for critical infrastructure companies. Under section 214 of the Homeland Security Act of 2002, if a company voluntarily submits critical infrastructure security information to the Department of Homeland Security, that information may not generally be disseminated or used for other purposes without the consent of the submitting party, so long as the information submission is accompanied by a statement electing coverage under this provision.¹⁶³ Section 214's nondisclosure provisions include a protection against dissemination and disclosure under the Freedom of Information Act, use of information in civil actions, or sharing of information with state and local authorities except for the express purpose of critical infrastructure protection.¹⁶⁴

However, the protections afforded under section 214 are constrained and, as such, offer little incentive to companies to audit their security systems. For example, section 214 only applies to information conveyed to the Department of Homeland Security. It does not apply to non-governmental, or non-DHS processes.¹⁶⁵ As such, section 214 offers no protection if a plaintiff seeks information directly from a company as part of a follow on negligence lawsuit. Similarly, section 214 does not preclude disclosure of information to the Congress.¹⁶⁶ Further, the section specifically provides that it does not preclude a federal, state or local agency from obtaining and using or disclosing the exact same information if it can be had under some other, independent means.¹⁶⁷ For example, if a company shares protected information with DHS, the Environmental Protection Agency could still seek, disclose and use (e.g., in an enforcement proceeding) the same information—albeit developed for a protected purpose—under another authority (e.g., the Clean Air Act).

A broader homeland security audit shield law (or series of laws at the state level) could greatly reduce the “ostrich problem.” This would remove a significant disincentive on management to regularly review and be fully aware of corporate homeland security performance. The information obtained in these audits—which would be much more operational in nature—could then serve as the basis for more general, better corporate homeland security SEC disclosures. This information, in turn, would allow a better informed market to act more effectively as a force for homeland security. Of course, any such law or laws would need to find an effective balance between the need for secrecy in the name of security and the public's right and need to know.

Information Sharing

In most cases, the information that would fall within SEC security disclosures requirements is already in corporate hands or could be obtained fairly easily through an internal or contracted-out vulnerability assessment or gap analysis. However, at present, some types of security information that would benefit shareholders are also unavailable to critical infrastructure companies.¹⁶⁸

A company cannot disclose what it cannot know; nor can a company be responsible for the nondisclosure of information it does not possess and/or is denied access to by responsible authorities.

A market-based disclosure regime will require a significantly improved two-way flow of information between DHS and other government agencies and the private sector. The legal/regulatory pressure on companies to disclose more information should also place similar pressure on DHS to be more open and less secretive. The SEC is in a position to help promote better dialogue and disclosure.

The Challenge of Foreign Ownership

The recent proposed sale of a series of important U.S. ports to Dubai Ports World, a United Arab Emirates-owned company, has brought a great deal of attention to the issue of foreign ownership of critical infrastructure. Some critics of the transaction are concerned that foreign owners of critical infrastructure might allow terrorists to utilize their holdings to attack the United States. While a market-based disclosure scheme cannot completely assuage these concerns, such a scheme would provide both a vehicle for greater oversight of the security of foreign-owned infrastructure and an impetus to encourage such owners to better secure critical infrastructure.

An SEC-based disclosure scheme only applies to publicly traded companies that are under the SEC's jurisdiction. Many foreign companies are outside these rules. However, a significant number of foreign companies are subject to specific SEC's rules as "foreign private issuers." Under current SEC rules, any foreign company that has more than 300 U.S.-resident holders of any class of security and total assets greater than \$10,000,000 must register and file certain disclosures with the SEC.¹⁶⁹ Many, if not most, foreign infrastructure companies fall within this provision and therefore would be subject to a SEC homeland security disclosure scheme. For example, **British Petroleum**, a U.K. company has extensive holdings within America's critical energy infrastructure and files with the SEC.¹⁷⁰ The French-owned company **Sodexo U.S.A.** is the nation's largest food service company, even providing services on domestic Marine bases; it, too, files with the SEC.¹⁷¹ Dubai Ports World, the company at the heart of the port controversy, does not currently file with the SEC as it is a state-owned enterprise.

Using SEC homeland security disclosures as a catalyst, the Congress could extend similar disclosures to all owner/operators of critical infrastructure, foreign and domestic, large and small. Such an extended scheme would provide a strong oversight mechanism over the nation's most vital infrastructure.

Conclusion

Terrorist organizations clearly have an on-going intention to attack our homeland by attacking our economy via our critical infrastructure. At the same time, there are strong indications that America's corporate sector is slipping back into complacency on matters of security. From a shareholder's standpoint, the security of an investment is substantially linked to the corporate security performance of the company and homeland security more broadly. The nation has a vital interest in encouraging—if not directly requiring—companies to do more to protect themselves and our critical infrastructure.

Generally speaking, there are few policy tools available to government decision makers to bring about better private sector homeland security. One such tool is the use of market-based measures. Market-based measures, whether on their own or in conjunction with other interventions, present a number of important policy advantages, including flexibility, immediate feedback, and cost-effectiveness. One readily available market-based measure for homeland security would be the wider and more effective

application of SEC disclosure requirements to homeland security matters.

Existing Securities laws likely already require companies to make material homeland security disclosures. However, the actual application of these provisions to homeland security matters is little understood and followed. Few companies disclose homeland security matters, even where such matters seem to be clearly within the scope of current disclosure requirements. Where such homeland security disclosures are made, they are generally inadequate for both the shareholder and national security. There is very little homeland security in securities.

In addition, the current status quo provides little incentive for better corporate homeland security, senior corporate management attention or public disclosure. The status quo actually works against those companies that take security concerns seriously. Such companies potentially face competitive disadvantage vis-à-vis competitors. This needs to change, since the terrorism threat to the United States will continue to exist and homeland security will only increase in importance.

The SEC has a number of courses of action available to bring about better disclosure of homeland security issues by public companies. These options range from putting public companies on notice that such disclosures are required under current rules to promulgating new requirements specific to homeland security. Any of these courses of action would be a significant improvement over the current practice. Disclosure can be an effective market-based tool to improve critical infrastructure security and protect our economy and society.

If the SEC seeks to bring about better disclosure of homeland security issues, it should tailor its action to focus companies on the types of homeland security information that would be most valuable to the companies themselves (as a vehicle for increasing management attention to these issues), to investors (as a vehicle for ensuring true security of their investments), and to the nation (as a vehicle for better homeland security).

About The Authors

Robert Housman is founder of and principal in The Housman Group. He is also Director of Legal and Regulatory Compliance for Resilient Corporation. He is a contributing author of the Homeland Security Law Handbook (Government Institutes 1993). From 1996 to 2001, he served as Assistant Director of Strategic Planning in the White House Drug Czar's Office. He has taught international law for American University's Law School and national security for Syracuse University's Maxwell School.

Timothy C. Olson currently serves as an advisor to Chesapeake Green Fuels. Prior to that, he worked for the Investigation Group International, the Chesapeake Bay Foundation and the Enforcement Division of the Securities and Exchange Commission. Mr. Olson is a graduate of Vermont Law School and Connecticut College.

Acknowledgements

The Center for American Progress is pleased to publish this abridged version of *New Strategies to Protect America: A Market-Based Approach to Private Sector Security* on behalf of its authors, Robert Housman and Timothy Olson. A more detailed version of the paper is available on the Center's website, www.americanprogress.org. The authors reserve all rights to both reports. Any use or reprint should include reference to the Center for American Progress as initial publisher of the report.

The authors wish to thank countless people who were generous with their time, critiques and thoughts in the preparation of this study. They extend special thanks to P.J. Crowley, senior fellow and director of national defense and homeland security, for bringing the project to fruition.

Endnotes

- 1 COUNCIL ON COMPETITIVENESS, CREATING OPPORTUNITY OUT OF ADVERSITY, PROCEEDINGS OF THE NATIONAL SYMPOSIUM ON COMPETITIVENESS AND SECURITY, 2003, at 8 [Council on Competitiveness 2003].
- 2 JOHN MOTEFF, CRS REPORT FOR CONGRESS, RL30153: CRITICAL INFRASTRUCTURES: BACKGROUND AND EARLY IMPLEMENTATION OF PDD-63, updated Sept. 2000, *available at* http://www.ncseonline.org/NLE/CRSreports/Science/st-46.cfm?&CFID=4361690&CFTOKEN=91384733#_1_16.
- 3 Robert Housman, Ed Bethune, *Birth and Development of Homeland Security Law*, in GOVERNMENT INSTITUTES, HOMELAND SECURITY LAW HANDBOOK, at 25-26 (2003).
- 4 Paul Magnusson, *Terror Threats: What Companies Need To Do*, BUSINESSWEEK, Aug. 16, 2004, *available at* http://www.businessweek.com/magazine/content/04_33/b3896042_mz011.htm.
- 5 THE CONFERENCE BOARD, REPORT #1333 CORPORATE SECURITY MANAGEMENT: ORGANIZATION AND SPENDING SINCE 9/11, July 9, 2003.
- 6 THE CONFERENCE BOARD, CORPORATE SECURITY MEASURES AND PRACTICES, MAR. 2005.
- 7 Information Week, *Midmarket Companies Get Serious About Security—For The Most Part*, Aug. 6, 2004, *available at* <http://informationweek.com/story/showArticle.jhtml?articleID=26806293>.
- 8 THE CONFERENCE BOARD, CORPORATE SECURITY MEASURES AND PRACTICES, MAR. 2005.
- 9 CIVITAS GROUP, THE HOMELAND SECURITY MARKET (2004).
- 10 It bears noting that in addition to governmental interventions, there are a limited number of private sector actions that can be undertaken to encourage better homeland security among critical infrastructure companies. For example, a host of private sector bodies can establish industry, or voluntary, standards for security. For example, the American Chemistry Council, the trade group of the major chemical companies has adopted a series of security standards in their existing Responsible Care program. Similarly, concerns about liability lawsuits, and actual lawsuits by injured parties, can compel significant changes in corporate behavior. Such lawsuits are typically private actions. There are governmental interventions that can raise (or reduce) the threat and viability of such lawsuits. For example, the Congress can statutorily reduce the burden of proof on plaintiffs. Alternatively, the Congress could statutorily impose a liability cap for companies that have adopted sound homeland security programs. However, at the end of the day, a liability regime is based upon private action—the threat that a private plaintiff will bring a lawsuit. These private sector mechanisms may play an important role in homeland security and deserve further analysis. However, they are not the focus of this report.
- 11 *See* COUNCIL ON COMPETITIVENESS, CREATING OPPORTUNITY OUT OF ADVERSITY, PROCEEDINGS OF THE NATIONAL SYMPOSIUM ON COMPETITIVENESS AND SECURITY (Oct. 2002), at 17, *available at* http://www.compete.org/pdf/c_and_s_report.pdf.

We must make security a core business value. Over the years, the private sector has built in quality, safety, health and productivity as essential, central elements of institutional culture and mission. Now security must become a part of the competitiveness equation . . . Only the private sector is able to design and implement solutions that embed security into business systems and processes.
- 12 *Id.* at 17.
- 13 SEC, Regulation S-K, 17 C.F.R. § 229.101.
- 14 *Id.* at § 229.303.
- 15 *Id.* at §229.101(c)(1)(xii). *See* Levine v. NL Industries, Inc., 926 F.2d 199, 203 (1991) - the cost of failing to comply with environmental regulations must be disclosed.
- 16 *Id.* at §229.103.
- 17 *Id.* at §229.303. The underlying purpose of MD&A is to provide investors with “information that the registrant believes to be necessary to an understanding of its financial condition, changes in financial condition and results of operations.” Item 303(a) of Regulation S-K [17 CFR 229.303(a)]. The SEC has also stated, “[i]t is the responsibility of management [in MD&A] to identify and address those key variables and other qualitative and quantitative factors which are peculiar to and necessary for an understanding and evaluation of the company.” SEC, Securities Act Rel. No. [6835](#), 54 Fed. Reg. 22427 (May 18, 1989) (*quoting* SEC, Securities Act Rel. No. 6349 (Sept. 28, 1981)).
- 18 *Id.*
- 19 SEC, Securities Act Rel. 33-6835, 54 Fed. Reg. at 22,430 (2002)
- 20 *See* Ottilie Jamel, Abigail Arms, MD&A 2005 Linchpin of SEC Post-Enron Disclosure Reform, SEC “Hot Topics” Institute Spring 2005, May 19, 2005, Washington, DC

- 20 GSE Systems Inc., Form10-K, 202, at 5 (2002).
- 21 LOCKHEED MARTIN CORPORATION, FORM 10-K 2004, at 19 (2004).
- 22 CACI INTERNATIONAL, AMENDMENT NO. 1 TO FORM S-3 REGISTRATION, at 34 (2002) .
- 23 Paul Pillar, *Is the Terrorist Threat Misunderstood?*, Security Management, May 2001, available at <http://www.securitymanagement.com/library/001116.html>.
- 24 Sean Mussenden, Henry Pierson Curtis, *No-Fly Zones Shield Disney's Resort*, ORLANDO SENTINEL, May 11, 2003 available at <http://www.globalsecurity.org/org/news/2003/030511-disney01.htm>.
- 25 WALT DISNEY COMPANY, FORM 10-K, 2004 (2004).
- 26 GMI, *Global Backlash Against US Brands*, Feb. 2, 2005, available at http://www.gmi-mr.com/gmipoll/press_room_wppk_pr_02022005.phtml. GMI's 2005 poll of 3,400 consumers across 20 nations found that McDonalds was the company most identified with the United States and which faced the second greatest problems as a result of that association.
- 27 Dan Murphy, *US Multinational Companies Wary of Backlash*, CHRISTIAN SCIENCE MONITOR, Apr. 21, 2003, available at <http://www.csmonitor.com/2003/0421/p12s01-woap.html>.
- 28 McDONALDS, FORM 10-K, 2004, at 25-26 (2004).
- 29 GMI, *Global Backlash Against US Brands*, Feb. 2, 2005, available at http://www.gmi-mr.com/gmipoll/press_room_wppk_pr_02022005.phtml.
- 30 ROBERT DACY, GAO, CRITICAL INFRASTRUCTURE PROTECTION; CHALLENGES AND EFFORTS TO SECURE CONTROL SYSTEMS, TESTIMONY BEFORE THE SUBCOMMITTEE ON TECHNOLOGY INFORMATION POLICY, INTERGOVERNMENTAL RELATIONS AND THE CENSUS, HOUSE COMMITTEE ON GOVERNMENT REFORM, GAO-04-628T, Mar. 30, 2004, at 5-6.

From 1995 through 2003, the CERT Coordination Center [the federal government's cyber-security center reported 12,946 security vulnerabilities that resulted from software flaws . . . Along with these increasing vulnerabilities, the number of computer security incidents reported to CERT/CC has also risen dramatically—from 9,859 in 1999 to 82,094 in 2002 and to 137,529 in 2003. And these are only the reported attacks. The Director of the CERT Centers has estimated that as much as 80 percent of actual security incidents goes unreported

- Id.*
- 31 *See, e.g.,* Alex Salkever, *The Ever-Growing Virus Crisis*, BUSINESSWEEK, Aug. 26, 2003, available at http://businessweek.com/technology/content/aug2003/tc20030826_4386_tc047.htm (damage estimates for the SoBig.f virus, which preyed on Windows' vulnerabilities ranged from \$550 to \$1 billion).
- 32 Gregg Keizer, *Worm Attack Could Rack Up \$50 Billion In U.S. Damages*, INFORMATIONWEEK, Jun. 4, 2004, available at <http://www.informationweek.com/story/showArticle.jhtml?articleID=21401700>.
- 33 MICROSOFT, FORM 10-K, 2004, at 16 (2004).
- 34 *Id.*
- 35 *See id.* at I.14,
- 36 GMI, *Global Backlash Against US Brands*, Feb. 2, 2005, available at http://www.gmi-mr.com/gmipoll/press_room_wppk_pr_02022005.phtml.
- 37 *See e.g.,* <http://www.inminds.co.uk/boycott-starbucks.html>; <http://www.zmag.org/content/showarticle.cfm?SectionID=&ItemID=1831>
- 38 BBC, *Blast Rocks North Beirut Suburb*, Aug. 22, 2005, available at http://news.bbc.co.uk/1/hi/world/middle_east/4175120.stm.
- 39 STARBUCKS, FORM 10-K, 2005, at 1 (2005).
- 40 *See* Bioterrorism Act, Pub. L. 107-188 (June 12, 2002); *see also*, FDA, Final Rule on Establishment and Maintenance of Records, 69 FR 71561, (Dec. 9, 2004).
- 41 Wal-Mart, *Wal-Mart At a Glance*, undated, available at <http://www.walmartfacts.com/newsdesk/wal-mart-fact-sheets.aspx#a125>.
- 42 George Anderson, *Wal-Mart Under Attack*, RETAILWIRE, Dec. 29, 2004, available at http://www.retailwire.com/Discussions/Sngl_Discussion.cfm/10345; Melissa Batulis, *Bomb Scare Shuts Down Ithaca Shopping Plaza*, WENY, available at <http://www.weny.com/News-Local.asp?ARTICLE3864=45469>; NBC10, *Police Say Man Spread Molotov Cocktails Around Wal-Mart*, Aug. 10, 2005, available at <http://www.nbc10.com/news/4835481/detail.html?subid=10101521>.
- 43 WAL-MART, FORM 10-K, 2005, at 14 (2005).
- 44 *Id.*

45 *See, e.g.*, Bioterrorism Act, Pub. L. 107-188 (June 12, 2002); USFDA/CFSAN, Guidance for Industry, Retail Food
Stores and Food Service Establishments: Food Security Preventive Measures Guidance, Final Guidance, Nov.
2003; USFDA/CFSAN, Retail Food Stores and Food Service Establishments: Food Security Preventive Measures
Guidance, Final Guidance, Nov. 2003; Field Instructions for Food Producers, Processors and Transporters: Food
Security Preventive Measures Guidance and Importers and Filers: Food Security Preventive Measures Guidance,
Mar. 2003.

46 UNITED AIRLINES, FORM 10-K, 2004, at unnumbered page (2005). The exact same discussion appears in United's
2004 Form 10-K. *See* UNITED AIRLINES, FORM 10-K, 2004, at unnumbered page (2004).

47 UNITED AIRLINES, FORM 10-K, 2004, at unnumbered page (2005). Again, the exact same discussion appears in
United's 2004 Form 10-K. *See* UNITED AIRLINES, FORM 10-K, 2004, at unnumbered page (2004).

48 DELTA AIRLINES, FORM 10-K, 2004, at 19-20 (2004).

49 DELTA AIRLINES, 2004 ANNUAL REPORT, at 8-9 (2004).

50 SOUTHWEST AIRLINES, FORM 10-K, 2004, at 3.

51 *Id.*

52 *Id.*, at 3 (2004).

53 CONGRESSIONAL RESEARCH SERVICE, CHEMICAL FACILITY SECURITY, July 29, 2005, at 14.

54 James Belke, Chemical Accident Risks in U.S. Industry-A preliminary analysis of accident risk data from U.S.
hazardous chemical facilities, Proceedings of the 10th International Symposium on Loss Prevention and Safety
Promotion in the Process Industries, Stockholm, Sweden, Pasman, Fredholm, and Jacobson (eds.), Elsevier (2001)
Science B.V. The EPA based this analysis on risk management plans submitted by facilities handling chemicals
covered by the section 112 of the Clean Air Act.

55 Lawrence Sherrod, *Chemical Security Ignites Capital Hill Combustion*, undated, available at http://www.gsnmagazine.com/jul_05/chemical_security.html.

56 *Id.*

57 *See* AP, Senate Mulls Chemical Plant Regulations, Dec. 2, 2005, available at <http://www.nytimes.com/aponline/business/AP-Chemical-Security-Threat.html?emc=eta1>.

58 US-PIRG, Dangerous Dozen, A Look at How 12 Chemical Companies Jeopardize Millions of Americans, Jun.
2004, available at <http://uspirg.org/reports/DangerousDozen2004.pdf>. While US-PIRG, is an advocacy group and
clearly not an objective research body, the group's analysis was subsequently relied upon by the Congressional
Research Service. *See* CONGRESSIONAL RESEARCH SERVICE, CHEMICAL FACILITY SECURITY, July 29, 2005, at 13, quoting
Carl Prine, *Chemicals Pose Risks Nationwide*, PITTSBURGH TRIBUNE-REVIEW, May 5, 2002, available at http://www.pittsburghlive.com/x/tribune-review/specialreports/potentialfordisaster/s_69664.html. It should be emphasized
that this report does not draw any conclusion as to whether these plants are among the nation's most deadly, nor
with respect to what level and sorts of harms could follow from an attack on these facilities. These reports are used
solely to raise the issue of what types of information companies perceived to be at risk to terrorism are disclosing
to their shareholders and the market. For the purposes of this report the ultimate accuracy of such reports is
nonconsequential.

59 *See* CLOROX CORP., FORM 10-K, 2004 (2004); DOW CHEMICAL CORP, FORM 10-K, 2004 (2004); PIONEER CHEMICAL
CORP., FORM 10-K, 2004 (2004); KIK CORP., FORM 10-K, 2004 (2004); Clean Harbors Corp., Form 10-K, 2004
(2004); DUPONT CORP., FORM 10-K, 2004 (2004); DOW CHEMICAL CORP., FORM 10-K, 2004 (2004);
FERRO CORP., FORM 10-K, 2004 (2004); OCCIDENTAL PETROLEUM CORP., FORM 10-K, 2004 (2004). One other public
company listed in the US-PIRG "Dirty Dozen," GATX is principally a leasing company. As a result, GATX's filings
are discussed in the rail section of this analysis. The other companies making up the dozen are privately held.

60 DUPONT, FORM 10-K, 2004, at 3 (2004). The company's 2005 10-K includes the same brief mention. DUPONT, FORM
10-K, 2005, at 3 (2005).

61 FERRO CORPORATION, FORM 10-K, 2004, at 3 (2004).

62 OCCIDENTAL PETROLEUM CORPORATION, FORM 10-K, 2004, at 33 (2004). Occidental is best known for its work in the
energy sector, however, the company also is active in the chemicals sector.

63 Sen. Joseph Biden, *When Chemicals Attack*, WASH. POST, Aug. 2, 2005, A13.

64 Joe Fiorill, *DC Train Ban Remains on Hold While Other Cities Efforts Advance*, www.GovExec.com, Aug. 11,
2005, available at <http://govexec.com/dailyfed/0805/081105gsn1.htm>.

65 CSX, 2004 ANNUAL REPORT, at 18-19 (2004); *see also* CSX, FORM 10-K, 2004, at 36 (2004).

66 *Id.* at 20 ("The inherent risks associated with safety and security, including adverse economic or operational effects
from terrorist activities and any governmental response").

67 UNION PACIFIC, FORM 10-K, 2004, at 34 (2004).

68 KC SOUTHERN, FORM 10-K, 2004, at 27 (2004). KC Southern provided:

The Company May Be Affected by Future Acts of Terrorism or War. Terrorist attacks, such as those that occurred on September 11, 2001, any government response thereto and war or risk of war may adversely affect the Company's results of operations, financial condition, and cash flows. These acts may also impact the Company's ability to raise capital or the Company's future business opportunities. The Company's rail lines and facilities could be direct targets or indirect casualties of an act or acts of terror, which could cause significant business interruption and result in increased costs and liabilities and decreased revenues. These acts could have a material adverse effect on the Company's results of operations, financial condition, and cash flows. In addition, insurance premiums charged for some or all of the coverage currently maintained by the Company could increase dramatically or certain coverage may not be available in the future.

Id.

- 69 BURLINGTON NORTHERN AND SANTA FE, FORM 10-K , 2004 at 37 (2004).
70 NORFOLK SOUTHERN CORPORATION, FORM 10-K, 2004 (2004). The SEC filings of the company's wholly owned rail subsidiary, Norfolk Southern Railway Company, also make no mention of terrorism. NORFOLK SOUTHERN RAILWAY COMPANY, FORM 10-K, 2004 (2004)
71 CANADIAN PACIFIC RAILWAY, FORM 10-K, 2004, at 22-23 (2004)
72 DHS, IAIP Directorate, Daily Open Source Infrastructure Report, for 03 December 2004, at p. 8

EMA drill tests hospital limits. A truck and three passengers contaminated with hazardous chemicals rolled into Chilton Medical Center in Clanton, AL, Tuesday afternoon, November 30, sending the Emergency Room (ER) into a state of emergency. The passengers were covered with aluminum phosphide pesticide and in a matter of 15 minutes they had contaminated five hospital personnel and the entire ER. Fortunately, the crisis was a drill on behalf of the Chilton County Emergency Management Agency (EMA).

Id.

- 73 Those who doubt that hospitals will be held to a standard of due care after a WMD attack should examine the case of the owners of the St. Rita nursing home in New Orleans. Thirty-four residents of the nursing home died when they were not evacuated in advance of Hurricane Katrina. The two owners of the facility have been charged with negligent homicide. See CNN, Nursing Home Owners Face Charges, Sept. 13, 2005, available at <http://www.cnn.com/2005/US/09/13/katrina.impact/>.
74 GAO, HOSPITAL PREPAREDNESS; MOST URBAN HOSPITALS HAVE EMERGENCY PLANS BUT LACK CERTAIN CAPACITIES FOR BIOTERRORISM RESPONSE, GAO-03-924, Aug. 2003, at 14-15.
75 HOSPITAL CORPORATION OF AMERICA, FORM 10-K, 2005, at 25 (2005).
76 TENET HEALTHCARE COMPANY, FORM 10-K, 2005, at 1 (2005)
77 *Id.*
78 Robert Hartwig, et. al, Insurance Information Institute, Terrorism, Insurance and the United States Government, Sept. 2004, at p. 1, available at http://server.iii.org/yy_obj_data/binary/741171_1_0/TerrorismInsurance.pdf.
79 *Id.*
80 RICHARD HILLMAN, GAO, TERRORISM INSURANCE; RISING UNINSURED EXPOSURE TO ATTACKS HEIGHTENS POTENTIAL ECONOMIC VULNERABILITIES, TESTIMONY BEFORE THE SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS, COMMITTEE ON FINANCIAL SERVICES, HOUSE OF REPRESENTATIVES, GAO-02-472T, Feb. 27, 2002.
81 *Id.* at p. 9-10.
82 *Id.*
83 *Id.*
84 Richard Leong, *Terror Insurance Cost Pits Lenders, Owners*, REUTERS, May 27, 2002.
85 GAO-02-472T, *supra* n. 140, at 12-13.
86 NIST, NCSTAR 1 (DRAFT), FEDERAL BUILDING AND FIRE SAFETY INVESTIGATION OF THE WORLD TRADE CENTER DISASTER, FINAL REPORT OF THE NATIONAL CONSTRUCTION SAFETY TEAM ON THE COLLAPSES OF THE WORLD TRADE CENTER TOWERS (DRAFT), at chap. 9 (published draft of June 23, 2005).
87 Laura McCallum, *Homeland Security Chief Meets with St. Paul Officials*, Minnesota Public Radio, July 22, 2005, available at http://news.minnesota.publicradio.org/features/2005/07/22_mccalluml_chertoff/ (quoting Secretary Chertoff saying "One of the things we want to be mindful of are those things that are potential targets because they

are national icons. . . and obviously the Mall of America has a national and international stature.”)

88 SIMON PROPERTY GROUP INC., FORM 10-K, 2003, at 68 (2003).
89 *Id.*, at 122.
90 RAMCO-GERSHENSON PROPERTIES TRUST, FORM 10-K, 2005, at exhibit 10.59 (2005).
91 HERITAGE PROPERTY INVESTMENT TRUST, FORM 10-K, 2004 at 17 (2004).
92 BOSTON PROPERTIES INC., FORM 10-K, 2005, at 21 (2005)(emphasis in the original).
93 *Id.*
94 EQUITY OFFICES PROPERTIES TRUST, FORM 8-K, 2004, at 7 (2004).
95 *Id.*
96 HOST MARRIOT, FORM 10-K, 2005, at 66-67 (2005).
97 STARWOOD HOTELS AND RESORTS WORLDWIDE, FORM 10-K, 2005, at 5 (2005).
98 See GAO, NUCLEAR REGULATORY COMMISSION: OVERSIGHT OF SECURITY AT COMMERCIAL NUCLEAR POWER PLANTS NEEDS
TO BE STRENGTHENED, GAO-03-752, Sept. 2003.
99 *A Review of Enhanced Security Requirements at NRC Licensed Facilities, Before the House Subcomm. on Oversight
and Investigations, Comm. on Energy and Commerce*, Apr. 11, 2002 (Testimony of David Orrick)(Capt. (ret.) Orrick is
a combat veteran who has led the Nuclear Regulatory Commission’s Operational Safeguards Response Evaluation
(OSRE) program since its inception in 1991), available at [http://energycommerce.house.gov/107/Hearings/
04112002hearing532/Orrick908.htm](http://energycommerce.house.gov/107/Hearings/04112002hearing532/Orrick908.htm).
100 GAO-03-752, n. 169, at 13-19.
101 Richard Perez-Pena, *Report Finds Security Flaws at Indian Point*, N.Y. Times, Dec. 8, 2002, available at [http://
www.nci.org/02NCI/12/nyt-08.htm](http://www.nci.org/02NCI/12/nyt-08.htm).
102 James Lee Witt Associates, *Review of Emergency Preparedness of Areas Adjacent to Indian Point and Millstone*,
2003.
103 Sandia National Laboratories, *Calculation of Reactor Accident Consequences-II Report*, 1982 (note these figures are
in 1982 dollars).
104 ENTERGY, FORM 10-K, 2004, at unnumbered page (2004). This list also includes the risk that the Indian Point facility
could be closed by regulatory authorities.
105 *Id.*
106 See generally, *id.*; see also Towers Perrin, *Workers Compensation Terrorism Reinsurance Pool Feasibility Study*,
April 2004, cited in Robert Hartwig, et. al, *Insurance Information Institute, Terrorism, Insurance and the United
States Government*, Sept. 2004, at 9 (\$15.4 billion in workers’ compensation losses alone).
107 EXELON CORPORATION, FORM 10-K, 2005 at 29 (2005)
108 *Id.*
109 GAO, *HOMELAND SECURITY: PRELIMINARY OBSERVATIONS ON EFFORTS TO TARGET SECURITY INSPECTIONS OF CARGO
CONTAINERS*, GAO-04-325T, Dec. 16, 2003,.
110 *Id.* at 3.
111 PricewaterhouseCoopers, *Cargo Security White Paper*, May 26, 2005, at 2.
112 See, *The Limitations of the Current Cargo Container Targeting, before the House Subcomm. on Oversight and
Investigations, Comm. on Energy and Commerce*, Mar. 31, 2004 (testimony of Commander. (ret.) Stephen Flynn).
113 See generally, 46 U.S.C. § 70103 (2204); see also United States Coast Guard, *National Maritime Security
Initiatives; Area Maritime Vessel, Facility, and Outer Continental Shelf Security; Automatic Identification System,
Vessel Carriage Requirement; Final Rules*, 33 C.F.R. §§ 101-106 (2005).
114 See *Final Rules*, *supra* n. 202, at § 105.
115 See 46 U.S.C. §§ 70108-70110 (2004).
116 GAO, *HOMELAND SECURITY: KEY CARGO SECURITY PROGRAMS CAN BE IMPROVED*, *supra* n. 197, at 20; *Addressing the
Shortcomings of the Customs-Trade Partnership Against Terrorism (C-TPAT) and the Container Security Initiative
(CSI), before the Senate Permanent Sub-Comm. on Investigations, Comm. on Homeland Security and Governmental
Affairs*, May 26, 2005 (testimony of Commander (ret.) Stephen Flynn).
117 Fareed Zakaria, *Does the Future Belong to China*, NEWSWEEK, May 9, 2005, available at [http://www.msnbc.msn.
com/id/7693580/site/newsweek/](http://www.msnbc.msn.com/id/7693580/site/newsweek/).
118 Adam Aston, et al, *From Choked Ports, Pricier Products*, BUSINESSWEEK, May 9, 2005, available at [http://www.
businessweek.com/magazine/content/05_19/b3932126.htm](http://www.businessweek.com/magazine/content/05_19/b3932126.htm).
119 Statement of Michael Laden, President, Target Customs Brokers, Inc., Minneapolis, Minnesota, on behalf of the
Retail Industry Leaders Association, Testimony Before the House Subcomm. on Trade, Comm. on Ways and Means,

June 15, 2004, available at <http://waysandmeans.house.gov/hearings.asp?formmode=view&id=1666> (Mr. Laden also testified in his capacity as President of Target Customs Brokers, Inc. a division of Target Corporation).
120 *Id.*
121 TARGET, FORM 10-K, 2005, at 18, exhibit 99C (2005)
122 *Id.*
123 Target Issues RFID Mandate, RFID Journal, undated, available at <http://www.rfidjournal.com/article/articleview/802/1/1/>.
124 SEASPAN, FORM F-1, 2005, at 27, available at http://www.seaspancorp.com/investor/sec_filings.html.
125 *Id.* at 22.
126 ALEXANDER & BALDWIN, FORM 10-K, 2004, at 22 (2004).
127 CP SHIPS, ANNUAL INFORMATION FORM 2004, at 5 (2004).
128 *Id.* at 36.
129 *Id.*

As a result of the significant insurance losses incurred in the September 11, 2001 attacks and related concern regarding terrorist attacks, insurers reduced or restricted coverage for terrorist losses generally. Accordingly, the level of terrorist coverage available to CP Ships was significantly reduced.

Id.
130 UPS, FORM 10-K, 2004, at 1 (2004).
131 *Id.*
132 *Id.*
133 *Id.*
134 *UPS Says Terrorism Disruption Cost \$130 Million*, EAST BAY TIMES, Sept. 28, 2001, available at <http://www.bizjournals.com/eastbay/stories/2001/09/24/daily60.html>.
135 GAO, AVIATION SECURITY: FEDERAL ACTION NEEDED TO STRENGTHEN DOMESTIC AIR CARGO SECURITY, GAO-06-76, Oct. 2005, at 46.
136 *See American ACADEMY OF ACTUARIES, TERRORISM INSURANCE COVERAGE IN THE AFTERMATH OF SEPTEMBER 11*, May 2002.
137 Dwight Jaffe, Thomas Russell, *Should Governments Support Private Terrorism Insurance Markets*, June 28, 2005, unpublished paper prepared for the WRIEC Conference, at 5, available at <http://faculty.haas.berkeley.edu/jaffee/Papers/DJTRSLCPaper.pdf>.
138 AMERICAN INTERNATIONAL GROUP, FORM 10-K, 2005, at 53 (2005).
139 *Id.* at 60. The 10-K also notes the impact of the 9-11 attacks on the airline industry and by extension AIG's aircraft financing operations. *Id.* at 79.
140 AON CORPORATION, 2004 ANNUAL REPORT (2004). Aon's 2005 Annual report was not available to the authors at the time of this writing.
141 AON CORPORATION, FORM 10-K, 2005, at 8 (2005).
142 Aon, *Private Insurance Market Cannot Operate Without Some Form of Public Backstop Against Catastrophic Terrorism Losses*, press release of Oct. 5, 2005, available at http://www.aon.com/about/news/press_release/pr_004DA6CD.jsp.
143 Dave Thomas, *9-11 Impact on Marsh Nothing Short of Devastation*, INSURANCE J., Sept. 6, 2004, available at <http://www.insurancejournal.com/magazines/east/2004/09/06/features/45941.htm>.
144 MARSH & MCLENNAN, 2004 ANNUAL REPORT, at 6 (2004); MARSH & MCLENNAN, FORM 10-K, 2004, at 19 (2004).
145 *See Cynthia A. Williams, The Securities and Exchange Commission and Corporate Social Transparency*, 112 HARV. L. REV. 1197, 1212-1223 (1999); *see also* LOUIS D. BRANDEIS, OTHER PEOPLE'S MONEY AND HOW THE BANKERS USE IT 92 (1914). ("Publicity is justly commended as a remedy for social and industrial diseases. Sunlight is said to be the best of disinfectants; electric light the most efficient policeman."); LOUIS LOSS & JOEL SELIGMAN, SECURITIES REGULATION 29 (3d ed. rev. 1998) ("Then too, there is the recurrent theme throughout [the federal securities laws] of disclosure, again disclosure, and still more disclosure. Substantive regulation has its limits. But 'the truth shall make you free.'")
146 Sarbanes-Oxley Act of 2002, Public Law No. 107-204 (July 30, 2002).
147 *See* Joshua A. Newberg, *Corporate Codes of Ethics, Mandatory Disclosure and the Market for Ethical Conduct*, 29 VT. L. REV. 253, 272-73 (2005).

The Sarbanes-Oxley Act of 2002 has been described as the most important change in U.S. securities regulation since the New Deal. Like the 1933 Securities Act and the 1934 Exchange Act, Sarbanes-Oxley was adopted in the wake of a crisis in securities markets. It contains a variety of measures aimed

at reducing the risks that public companies will “implode in a wave of accounting scandals” of the type that brought down Enron, threatened other large U.S. corporations, and cast doubt over the integrity of information disclosed by companies listed on U.S. securities markets. . . . [T]he Sarbanes-Oxley Act mandates, among other things: disclosure in annual reports of material off-balance sheet transactions that may affect the issuer’s financial condition; creation of a new U.S. Public Company Accounting Oversight Board; inclusion of a financial expert on an issuer’s audit committee; trading blackout periods for executives and directors when other employees are subject to blackout periods in connection with their participation in defined contribution pension plans; certification by CEOs and CFOs of the accuracy of annual or periodic reports filed with the SEC; and disgorgement by CEOs and CFOs of certain compensation if financial reports are restated.

Id. at 272-73 (citations omitted).

148 *See e.g.* Susannah Blake Goodman & Tim Little, *The Gap in GAAP: An Examination of Environmental Accounting Loopholes 17* (Dec. 2003) (unpublished manuscript on file with The Rose Foundation for Communities and the Environment – Environmental Fiduciary Project at www.rosefdn.org).

Essentially, what Sarbanes-Oxley did was to increase scrutiny of corporate financial disclosures and raise the stakes for non-compliance with GAAP and SEC disclosure regulations. Although the full implications of Sarbanes-Oxley are still being debated and aspects of it may ultimately be resolved in the courts, it is generally accepted that the Sarbanes-Oxley Act mandates that public companies should establish and maintain disclosure controls and procedures that continually generate and provide to the chief executive officer and chief financial officer all information required for accurate disclosure purposes. It also made the CEO and CFO personally responsible for the accuracy of the registrants’ filings, and increased the independence and responsibility of the audit committee to ensure the integrity of corporate financial information collection and reporting systems.

Id. at 17.

149 ARC Strategies, *Linking Supply Chain Security with Sarbanes-Oxley and The Bottom Line*, Aug, 2004, at 7.

150 *See e.g.* Ann R. Barker, *Environmental Management Systems After Sarbanes Oxley 4* (2004) (unpublished manuscript on file with Integrated Petroleum Environmental Consortium (IPEC), *available at* http://ipec.utulsa.edu/Ipec/Conf2003/Papers/barker_27.pdf).

Prior to SOX disclosure requirements were primarily focused on material claims or proceedings, and companies employed varying approaches for determining and reporting environmental liabilities. Now companies must also be concerned about the accuracy of the financials and whether systems are in place to assure accuracy of the financials and authenticity of corporate attestations. Given the increasing scrutiny surrounding financial disclosure, efforts to present these liabilities in their most favorable light while balancing environmental regulations and SEC rules may no longer be reasonable or possible.

Id. at 4.

151 *See, e.g.*, CERES, *Corporate Governance and Climate Change*, *available at* <http://www.ceres.org/pub/publication.php?pid=45>.

152 SEC, Securities Act Rel. Nos. 33-8040; 34-45149. The Cautionary Advice noted:

We have observed that disclosure responsive to these requirements could be enhanced. For example, environmental and operational trends, events and uncertainties typically are identified in MD&A, but the implications of those uncertainties for the methods, assumptions and estimates used for recurring and pervasive accounting measurements are not always addressed.

Id.

153 While materiality is driven by the bottom line, the SEC has indicated that companies should not adopt a hard, fast, qualitative, or percentile, “rule of thumb.” *See* SEC Staff Accounting Bulletin No. 99, *available at* www.sec.gov/interp/account/sab99.htm.

154 SEC, Regulation S-K, 17 C.F.R. § 229.101.

155 *Id.* at § 229.103.

156 *Id.* at § 229.303.

157 SEC, Securities Act Rel. No. [6835](#), 54 Fed. Reg. 22427(May 18, 1989).

158 *See* Richard A. Posner, *Our Incompetent Government*, *THE NEW REPUBLIC*, Nov. 14, 2005 (“The human mind finds it difficult to think in terms of probabilities, as distinct from frequencies, and often solves its difficulty

by writing them down to zero. If an event is frequent, people expect it to recur. But if you tell them something that has not occurred might occur and if it does occur it will cause great loss, they are likely to be unimpressed Americans are not fatalists Americans simply do not accept the inevitability of disaster.”)

159 See Sarah Stafford, Explaining State Adoption of Environmental Audit Legislation, unpublished paper, Mar. 2004, at 4, available at http://slstaf.people.wm.edu/Stafford_State_Adoption.pdf; John A. Lee & Bertram C. Frey, Environmental Audit Immunity Laws: A State-by State Comparison, ENVTL. REP. (BNA), July 9, 2004, at S-3.

160 See EPA, ‘Incentives for Self- Environmental Audit Immunity Laws: A State-by State Comparison, Policing: Discovery, Disclosure, Correction and Prevention of Violations, 60 Fed. Reg. 66706 (Dec. 22, 1995), as modified, EPA, Incentives for Self-Policing: Discovery, Disclosure, Correction and Prevention of Violations; Notice, Final Policy Statement, 65 Fed. Reg. 19617 (Apr. 11, 2000).

161 EPA, Incentives for Self-Policing: Discovery, Disclosure, Correction and Prevention of Violations; Notice, Final Policy Statement, 65 Fed. Reg. 19617 (Apr. 11, 2000).

162 See Sarah Stafford, *Does Self-Policing Help the Environment? EPA’s Audit Policy and Hazardous Waste Compliance*, 6 VT J. ENVTL. L. (2004-2005).

163 Homeland Security Act of 2002, Pub. L. No. 107-296, § 214 (2002), 6 U.S.C. §133

164 *Id.*

165 *Id.* at §214(a).

166 *Id.* at §214(d)(ii)(I).

167 *Id.* at §214(c).

168 *Accord*, GAO, HOMELAND SECURITY: INFORMATION SHARING RESPONSIBILITIES, CHALLENGES, AND KEY MANAGEMENT ISSUES, GAO-03-715T, May 8, 2003, at 25.

169 SEC, Exchange Act Rule 12g-4(a)(2); 17 C.F.R. 240.12g-4(2) . The SEC, however, has proposed new rules that would allow more foreign companies to avoid having to file as foreign private issuers. Securities Act Rel. No. 34-53020 (Dec. 27, 2005).

170 BP P.L.C., FORM 6-K (Mar. 13, 2006).

171 See, e.g., SODEXHO ALLIANCE, SA, FORM 6-K, (Jan. 2006).

Center for American Progress



ABOUT THE CENTER FOR AMERICAN PROGRESS

The Center for American Progress is a nonpartisan research and educational institute dedicated to promoting a strong, just and free America that ensures opportunity for all. We believe that Americans are bound together by a common commitment to these values and we aspire to ensure that our national policies reflect these values. We work to find progressive and pragmatic solutions to significant domestic and international problems and develop policy proposals that foster a government that is “of the people, by the people, and for the people.”

Center for American Progress
1333 H Street, NW, 10th Floor
Washington, DC 20005
Tel: 202.682.1611 • Fax: 202.682.1867
www.americanprogress.org