SOLVING THE INFORMATION SECURITY & PRIVACY CRISIS BY EXPANDING THE SCOPE OF TOP MANAGEMENT PERSONAL LIABILITY

Charles Cresson Wood†

ABSTRACT

While information security and privacy losses are now spiraling out of control, and have been demonstrably shown to threaten national sovereignty, military superiority, industrial infrastructure order, national economic competitiveness, the solvency of major businesses, faith and trust in the Internet as a platform for modern commerce, as well as political stability, the U.S. Congress has nonetheless to date refused to seriously address the root cause of these threats. The root cause is a legally reinforced incentive system that encourages, and further entrenches, top management decisions that provide inadequate resources for, and inadequate top management attention to, information security and privacy matters. This article explains why the current top management legally defined incentive systems are dysfunctional and how they should be modified so as to create considerably more socially desirable results. Employing a minimum-changes politically palatable strategy, the article discusses how a revival of the common law theories of negligence and recklessness, in both the criminal and civil areas, can be used to establish a new socially beneficial top management incentive system. A draft federal statute manifesting these recommendations is provided.

INTRODUCTION

The information security and privacy crisis that the world now faces is so shocking, so damaging, and so pervasive, that it seems impossible to resolve. But this viewpoint, which is widely disseminated in the mass media, is, in fact, reasonable only when the root cause of the crisis is not understood. In reality, the crisis is repeatedly being entrenched, perpetuated, and worsened by top management incentive systems that strongly discourage top managers from giving this area the attention it must have, and from making the investment that this area requires. In other words, the current legally defined top management incentive system keeps us in a vicious circle that perpetuates the status quo, which is clearly not working.

While top management's fiduciary obligations to the organization where they work do promote decisions for the benefit of the organization and its primary

†JD, MBA, MSE, CISM, CISSP, CISA, Independent Information Security & Privacy Consultant. Special thanks to Carol J. Buckner, Dean at St. Francis School of Law, for her astute suggestions and directions. Thanks are also extended to reviewers Jacques Francoeur, Barbara Ellen Auerbach, Douglas P. Feil, Mark A. Lemley, and Martin D. Finch.

constituencies such as shareholders, donors, and taxpayers, the legally recognized duty of care to which top management must comply does not promote top management's observation of duties to third parties such as current customers, ex-employees, and existing business partners. For example, the typical current top management incentive systems encourage secrecy, conflicts of interest, short-term decisions, excessive risk taking, and grossly inadequate investment in the infrastructure needed to achieve adequate levels of information security and privacy.

The world has changed dramatically, thanks to powerful new technologies like the Internet and mobile computing, and citizens of industrialized nations are now much more connected. The law needs to reflect this interconnectedness by using a consistent and standardized nation-wide approach (and later a world-wide approach).

Recognizing that top managers, at least in the information security and privacy area, have become stewards of the public trust, the ones to make decisions that materially affect third parties, this article proposes that we push the reset button in the law. It suggests that we revert to time-tested and proven traditional tort concepts of negligence and recklessness (both civil and criminal). Relevant defenses, notably the business judgment rule, the assumption of the risk defense, the contributory negligence defense, and the license defense, are also in need of material change to acknowledge the new reality which requires a more socially responsible standard of conduct to which top management must legally adhere.

Using a new model law as a reference point, the author suggests that with a minimum number of conservative changes to existing laws, the U.S. Congress can establish a new and truly motivating level of top management personal liability for information security and privacy harms done to third parties. With such a federal law, the Congress could thereby rapidly bring about considerably more socially desirable results, including enhanced trust in the economic and technological infrastructure, and a marked reduction in the level of losses currently sustained.

I. TOP MANAGEMENT INCENTIVE SYSTEMS ARE A CRITICAL DETERMINANT OF INFORMATION SECURITY & PRIVACY LOSSES

Reeling from widespread criticism that it has coddled Wall Street criminal bank executives,[1] demonstrated by the fact that not a single indictment of an executive has been handed down since the disastrous financial crisis of 2007-2008, the U.S. Justice Department has recently issued new policies that prioritize the prosecution of individual employees, not just the companies where they work.[2] While major

1. David Michaels, *2015 Spurred Billions in Bank Fines, But Not Enough for Warren*, BLOOMBERG BUSINESS (Jan. 29, 2016), http://www.bloomberg.com/news/articles/2016-01-29/2015-spurred-billions-in-bank-fines-but-not-enough-for-warren (discussing recent Wall Street fraud prosecutions in which no individual bank executives were prosecuted by the government).

2. Matt Apuzzo & Ben Protess, *Justice Department Sets Sights on Wall Street Executives*, N.Y. TIMES (Sept. 9, 2015), http://www.nytimes.com/2015/09/10/us/politics/new-justice-dept-rules-aimed-at-prosecuting-corporate-executives.html?emc=eta1&_r=0. This policy represents an acknowledgement by the federal government that the current top management incentive system is in need of adjustment, the same topic that this article addresses.

fines related to that financial crisis have been levied against involved corporations, there is a serious danger that these fines will simply be viewed as a routine cost of doing business, and so the current dangerous, risk-seeking behavior will not change. To avoid continuing, serious, and socially detrimental results, the legal incentive systems surrounding executive responsibility urgently needs to be realigned so as to reflect greater executive personal responsibility for decisions that affect third parties.[3] This is true in the financial sector, as evidenced in the propensity to take on excessive debt, and it is true in the domain of information security and privacy, as evidenced by many dramatic recent headlines.[4]

Corporations do not commit crimes, do not have a mind that could generate malicious intent, do not act negligently, and do not, in and of themselves, cause material losses to others. Corporations are simply an organizational form through which people act; they are not a culpable party. Fines levied against corporations alone will therefore not have significant motivational effects. But rather than pinning responsibility on specific executives, the U.S. justice system typically shields top management using traditional agency law theories and the business judgment rule. To compel top management to pay more attention to the pressing information security and privacy crisis that the nation now faces, and to force top managers to allocate sufficient resources to adequately and responsibly deal with this serious problem, a realignment in the U.S. legal incentive system is now required. That sought-after incentive system realignment can be achieved by: (1) updating the laws of negligence and recklessness to enable and facilitate lawsuits brought by third parties who have been seriously harmed by personally-responsible top management, (2) recognizing a type of white-collar managerial crime in the law, a genre of criminal negligence or recklessness, which acknowledges that, when it comes to information security and privacy, corporate top managers are now important stewards of the public trust, and (3) limiting the use of certain defenses, such as the business judgment rule and the assumption of risk, that would prevent charges of negligence and recklessness from being illegitimately blocked in court proceedings by defense counsel.

This article will explore the nature of the current information security and privacy crisis and note some aggravating forces that will continue to cause the crisis to get worse—that is, unless these forces are reversed by changes in incentive-system-related law, such as those described herein. The article will additionally explore who actually makes decisions about information security and privacy in organizations, and the primary incentive systems now causing these parties to act in ways that are seriously dysfunctional. After a brief history of top management

---

3. Public opinion is in support of such a change in the law, and top-level business leaders agree. A study done by the New York Stock Exchange Governance Services, noted that nine out of ten board of director member respondents believed that businesses should be held liable if they do not abide by the standard of due care. *See NYSE & Veracode, Cybersecurity and Corporate Liability: The Board's View,* VERACODE 2 (Nov. 5, 2015), https://www.veracode.com/nyse-and-veracode-survey-reveals-cyber-related-corporate-liability-is-top-of-mind-for-boards-and-executive.

4. The appropriate level of executive personal liability for harms caused to third parties is certainly not a conversation unique to the United States. For example, there has been increasing liberalization of the rules allowing shareholder derivative suits against top management in Japan since the 1990s. *See* Carl F. Goodman, *The Somewhat Less Reluctant Litigant: Japan's Changing View Toward Civil Litigation*, 32 L. & POL'Y INT'L BUS. 769, 799 n.131 (2001).

personal liability for information security and privacy harms caused to third parties, the article goes on to define a new "standard of care,"[5] a readily achievable standard to which top management should conform in order to avoid personal civil liability and/or criminal culpability.

The specific changes to agency law and the business judgment rule that are necessary to successfully bring about this change in incentives are also covered. To clarify exactly what is required and simplify the determination of whether a tort or a crime has taken place, the article will also suggest a safe harbor provision that will allow top management to readily determine whether they are on the right side of the law. Thus, top management decision-related operational simplicity, low cost to implement, low cost to determine potential liability, and low cost to adjudicate/ settle, have been significant objectives in the drafting of the model law found in the appendix to this article.

While other aspects of the law of executive responsibility and accountability related to information security and privacy clearly need to be changed,[6] this article focuses only on executive responsibility and accountability because that area is so key to remediating the pressing crisis we now face.[7] Using conservative and modest changes and realignments to traditional and well-established concepts of the law related to liability and personal responsibility, this article proposes a relatively inexpensive, relatively easy to implement, and relatively minor set of adjustments to the law that are likely to have a significant and long-lasting effect in terms of: (1) preserving the integrity and resilience of both information systems and societal infrastructure managed by information systems, (2) maintaining and enhancing national competitiveness, and (3) protecting and enhancing national security. Trust is an essential factor that must be present if a populace will allow the government to govern them. It must additionally be present if a customer is to engage in a sale with an online business. Trust in both our current legal system and our current

5. The common law surrounding negligence for information security and privacy matters is already tending in the direction proposed in this article, although it needs to be advanced and clarified, for example, through the statute proposed in the appendix. Consider Byrne v. Avery Ctr. for Obstetrics and Gynecology, 102 A.3d 32 (Conn. 2014), which involved the Connecticut Supreme Court recognizing that the controls found in regulations implementing the Health Insurance Portability and Accountability Act ("HIPAA") constitute a standard of due care that could be referenced for purposes of determining negligence.

6. Certainly, other significant changes are needed in addition to a shift in the legal definition of executive personal responsibility. For example, the U.S. Justice Department must stop using deferred prosecution agreements ("DPAs") and non-prosecution agreements ("NPAs") to prevent corporations from running the risk that, after a criminal conviction, they will be branded as criminals and then suffer a major erosion in their reputation. *See* Russell Mokhiber, *Twenty Things You Should Know About Corporate Crime*, 25 CORP. CRIME REP. 25 (2007). Another major change that is needed is that vendors that sell information security and privacy products that are clearly insufficiently secured need to be held strictly liable for the damage that their products cause. *See* Michael D. Scott, *Tort Liability for Vendors of Insecure Software: Has the Time Finally Come?*, 67 MD. L. REV. 425 (2008); David Sirota, *Prosecution of White Collar Crime Hits 20-Year Low*, ALTERNET (Sept. 10, 2015), http://www.alternet.org/news-amp-politics/prosecution-white-collar-crime-hits-20-year-low.

7. Increased top management personal liability as discussed in this article is fully consistent with provision 404(b) found in the Sarbanes-Oxley Act of 2002. That provision requires top management to assess and attest to the financial control measures used to prepare the financial statements for public companies. The American Institute of Certified Public Accountants ("AICPA") believes that the law has led to improved financial reporting and greater transparency. This article seeks to move in that same general direction, but in the domain of information security and privacy. *See* Section 404(b) of Sarbanes-Oxley Act of 2002, AM. INST. OF CPAS, http://www.aicpa.org/Advocacy/Issues/Pages/Section404bofSOX.aspx.

technological structure is now in serious jeopardy and urgently needs to be bolstered and augmented. The proposed law in this article attempts to serve that objective of enhancing trust as well.

The law of unintended consequences[8] holds that "the actions of people, particularly the actions of the government, always have effects and consequences that are unanticipated."[9] Although politicians often ignore that law, this author has consistently borne it in mind, and employed great caution when preparing the limited changes in the law described below. This article does not so much advocate a new approach, as it suggests that various traditional tried-and-true legal approaches, approaches that have been demonstrably workable in the traditional system of common law, can be combined in a different way to achieve socially desirable results, notably achievement of an adequate level of information security and privacy. Accordingly, the limited-scope and most-conservative recommended changes in the law described in this article are fundamentally (a) explicit definitions of matters that remain vague in the law, (b) new applications of existing common law and statutes, and (c) limitations of the defenses provided by existing laws.

II. COMPELLING EVIDENCE NOW SHOWS THAT WE ARE IN AN INFORMATION SECURITY AND PRIVACY CRISIS

That America is in serious trouble can firstly be shown by the April 2015 breach of computers at the U.S. Office of Personnel Management.[10] That security breach resulted in personally identifiable information such as names, Social Security numbers, dates of birth, and addresses, being released for millions of people who had undergone military and government agency background checks. Not only does the breach pose a short-term risk of identity theft, but it will jeopardize U.S. undercover operations for a generation since those involved will be subject to blackmail, unexpected disclosure of their identities, etc. That one attack changes the balance of power between countries, alters the battlefield of international conflicts, and jeopardizes American competitiveness. That attack also points to the fact that computers and networks are the modern nervous system of our society, and they must be vigorously and effectively protected, if our now highly automated society is going to survive.

That the nation is now in a serious information security and privacy crisis can secondly be illustrated by the Sony Pictures Entertainment attack that took place on November, 24, 2014.[11] As a result of that attack, a major corporation lost the use of

---

8. Although certainly much older in its origins, this law was popularized by sociologist Robert K. Merton. *See* Michael T. Kaufman &Robert K. Merton, *Versatile Sociologist and Father of the Focus Group, Dies at 92,* N.Y. TIMES (Feb. 24, 2003), http://www.nytimes.com/2003/02/24/nyregion/robert-k-merton-versatile-sociologist-and-father-of-the-focus-group-dies-at-92.html.

9. Rob Norton, *Unintended Consequences*, LIBRARY OF ECONOMICS AND LIBERTY (2002), http://www.econlib.org/library/Enc/UnintendedConsequences.html.

10. David E. Sanger & Julie Hirschfeld Davis, *Hacking Linked to China Exposes Millions of U.S. Workers,* N.Y. TIMES (June 5, 2015), http://www.nytimes.com/2015/06/05/us/breach-in-a-federal-computer-system-exposes-personnel-data.html.

11. Lori Grisham, *Timeline: North Korea and the Sony Pictures Hack*, USA TODAY (Jan. 5, 2015), http://www.usatoday.com/story/news/nation-now/2014/12/18/sony-hack-timeline-interview-north-korea/20601645.

over 3,000 computers and 800 servers. All connections to the Internet were shut off, including connections to other Sony units and third parties. The corporation was plunged into a pre-digital age of landline telephone and hand-delivered messages written via pen and paper. Not long after that, President Barack Obama declared a national emergency[12] and issued an executive order to deal with the "increasing prevalence and severity of malicious cyber-enabled activities originating from, or directed by persons located, in whole or in part, outside the United States."

In other words, the game has recently changed and nation states are now actively engaged in cyber-warfare, and both corporations and government agencies are at significant risk. While those seeking to make political points ("hacktivists"), those seeking to show their intellectual prowess ("hackers"), as well as those seeking to "make a buck" from crimes such as identity theft ("ghosts"), are certainly still serious concerns, the attackers now include agents from well-financed nation states and operatives from sophisticated organized crime gangs.[13]

While there is unquestionably a wide variety of very powerful and versatile new security and privacy technology available, the fundamental issue behind information security and privacy problems that we now experience involves people.[14] Technology alone is not going to solve information security and privacy problems. Instead, management must devote additional attention to the risks that new information systems like the Internet introduce, and they must also allocate sufficient resources so that these same security and privacy problems can be adequately addressed. Top management now stands as the gatekeeper, holding the purse strings of organizations, and it is often blocking the work on information security and privacy that must be undertaken in order to adequately protect information systems, as well as the assets, both physical and intellectual, that these information systems control. Unfortunately, the prevailing incentive systems, such as quarterly bonuses paid for high profits, encourage top management to act in a penny-pinching manner, denying these essential activities both the top management attention and the resources that these areas must now receive.[15]

III. CURRENT INCENTIVE SYSTEMS CAUSE TOP MANAGEMENT TO INADEQUATELY ADDRESS INFORMATION SECURITY AND PRIVACY

A. Top Management Does Not Personally Pay the Price for Insufficient Information Security & Privacy

Like all people in America today, top managers are operating in the midst of a

12. Exec. Order No. 13694, 80 Fed. Reg. 18077, 18077 (Jan. 6, 2015). Reflecting the serious problems in this area, one should note that President Obama has issued a total of five Executive Orders and Presidential Directives that authorize offensive and defensive actions in cyberspace. *See* Catherine A. Theohary & Anne I. Harrington, *Cyber Operations in DOD Policy and Plans: Issues for Congress*, 22 CONGRESSIONAL RESEARCH SERVICE, (Jan. 5, 2015), https://fas.org/sgp/crs/natsec/R43848.pdf.

13. Jeremy Bergsman, *Do You Care Who's Attacking Your Firm?,* CEB BLOGS (May 13, 2015), https://www.cebglobal.com/blogs/information-security-do-you-care-whos-attacking-your-firm.

14. *See* Donn B. Parker, *People Are the Number One Problem for Computer Security: Some Suggestions for Control*, 2 COMPUTER CRIME DIG. 5, 5-10 (1984).

15. Gary Loveland & Mark Lobel, *Cybersecurity: The New Business Priority,* PRICEWATERHOUSECOOPERS, http://www.pwc.com/us/en/view/issue-15/cybersecurity-business-priority.html.

complex modern social system, and are thus subject to influence from a variety of objectives, incentives, and constraints.[16] Beyond their own personal objectives and personalities, the behavior of top management can be predicted to be a function of those same objectives, incentives, and constraints. For example, if (thanks to limited corporate liability laws) top management at a high-tech venture-capital-funded firm is playing with other people's money, and their own net worth will not be adversely impacted if a serious security or privacy problem were to occur, top management will be encouraged to take on an excessive level of risk in the hope that they might hit it big with the new firm.[17] So if the budget allocation for information security and privacy is insufficient, and a serious loss does later result, top management does not generally personally pay the price.[18] The price is instead paid by the organization, and/or third parties such as suppliers and in some instances, investors, customers, and the general public. Since top managers personally enjoy the benefits of a restricted budget for information security and privacy, via higher quarterly bonuses,[19] more promotions, etc., and because top management can spread the costs across third parties (economists call the effects of this spreading "externalities"[20]), top management is now economically encouraged to keep information security and privacy budgets dangerously low.[21]

---

16. PAULINE BOWEN ET AL., INFORMATION SECURITY HANDBOOK: A GUIDE FOR MANAGERS (Nat'l Inst. of Standards and Tech.) (2006).

17. Top managers know more about risks facing the organization than investors or other parties, and this asymmetry of knowledge encourages top managers to take on excessive risks. This problem has been widely studied. *See* Peter M. DeMarzo et al., *Risking Other People's Money: Gambling, Limited Liability, and Optimal Incentives*, Working Paper No. 3149, STANFORD GRADUATE SCHOOL OF BUSINESS (2014), *available at* https://www.gsb.stanford.edu/faculty-research/working-papers/risking-other-peoples-money-gambling-limited-liability-optimal.

18. As one illustrative recent case, consider the massive release of credit card numbers that Target experienced on December 19, 2013. *See* Brian Krebs, *The Target Breach, by the Numbers*, KREBS ON SECURITY (May 14, 2014), http://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers. Some 70 million credit card numbers were stolen, and those cardholders had an unknown amount of expenses associated with changing cards, at the very least. *Id*. The banks that issued the credit cards paid an estimated $200 million to reissue the credit cards. *Id*. Target itself will be spending $100 million to upgrade its point of sale terminals to support the new Chip-and-PIN technology. *Id*. Target also paid a $10 million settlement for a class action lawsuit brought by customers, and a $67 million settlement to Visa and its card issuers. *Id*. Target laid off 1,700 employees because sales were down as a result of the breach. *Id*. The CEO stepped down from his position, but he stands to reap $55 million from an executive compensation golden parachute package. *Id*. A shareholder derivative suit was filed in the District of Minnesota on January 29, 2014, named Collier v. Steinhafel et al., No. 14-cv-266 (D. Minn. Jan. 29, 2014), but according to this author's analysis of PACER records, which was performed on February 8, 2016, there have been no notable developments since.

19. Alfred Rappaport, *Executive Incentives vs. Corporate Growth*, HARV. BUS. REV., (July-Aug. 1978), *available at* https://hbr.org/1978/07/executive-incentives-vs-corporate-growth. In this classic article, Rappaport describes how incentive systems focused on short-term earnings encourage short-term thinking by top management. *Id*.

20. For a discussion of the perverse behind-the-scenes effects associated with inadequate investment levels in information security, including externalities, *see* Ross Anderson, *Why Information Security Is Hard—An Economic Perspective*, 358 (2001) (unpublished manuscript), https://www.acsac.org/2001/papers/110.pdf.

21. *See* SYDNEY FINKELSTEIN ET AL., STRATEGIC LEADERSHIP: THEORY AND RESEARCH ON EXECUTIVES: TOP MANAGEMENT TEAMS, AND BOARDS 336 (2009) (discussing how top management adjusts strategic behavior to manipulate measures of their performance).

B. Information Security and Privacy Requires Exceedingly Complex Long-Term Investment in Control Systems

At the same time, computer systems and networks are some of the most complex things that humans have ever created. To manage them adequately, notably to keep them properly secure and private, top management must establish and maintain exceedingly complex control systems. The development and use of these control systems requires a long-term effort that requires an incredible amount of both management attention and resources. The computer systems and networks that our society is now so dependent upon are the result of decades of compounded growth, where the older technologies have been augmented by newer technologies. As a result of this adding-on process, various problems are introduced, including gaps in knowledge, lapses in controls, inconsistencies, irregularities, and incompatibilities, and these problems in turn have often led to security and privacy losses. The many layers of inconsistent technological systems that now exist are revealed by the plugs and jacks used to connect various types of computers and mobile computing devices. In this environment, even a layperson can get a sense for the irregularity, non-standardization, inconsistency, and lack of coherence in many information systems today.

Since top management is now rewarded primarily based upon short-term financial performance, they have a disincentive against investing in the long-term control systems necessary to bring coherence, consistency, organization, security, and privacy to these information systems.[22] As a consequence, top management helps to create long-term information security and privacy risks of immense proportion that only get more dangerous, pervasive, and more systemic as time goes on. In order to stop these risks from growing still more disastrous and pervasive, a change in the legal system that recognizes top management personal liability for harms done to third parties is now required.

C. Stock Options Create Short-Term Focus Incompatible with Investment in Long-Term Technology Infrastructure

The pervasive use of stock options, as a part of a typical private sector top management compensation package, creates many of the same dysfunctional results as bonuses based on quarterly financial results. The ensuing focus on stock price brings a short-term viewpoint that encourages short-term thinking, and short-term strategies. This focus will hopefully hold up at least until the top level manager instituting them has retired, has taken a job at another organization, or has died. Since information security and privacy requires a significant dedicated long-term investment in order to be done successfully, to the extent that chief executives are

22. Since complexity management is a significant causal factor behind a wide variety of information security and privacy problems (such as errors in setting-up access control permissions), top management must take the time, and invest the resources, to deal with complexity management issues if they are going to adequately address information security and privacy. *See* Mark Mitchell, *Reducing Complexity, Ensuring Security: Toward Better Information Management*, Government Executive (Aug. 20, 2014), http://www.govexec.com/insights/reports/reducing-complexity-ensuring-security-toward-better-information-management/91952.

paid with stock options, this arrangement further supports their focus on short-term financial results,[23] which can and often does have dysfunctional impacts on the necessary long-term investment in technological infrastructure, such as in information security and privacy.[24]

Options are inherently speculative. When an organization bases a large part of a top manager's pay on a speculative matter, the organization should not be surprised that the top manager is taking a high-risk bet. Top managers should be required to hold options for a long period of time, such as a decade or two, so as to foster long-term investment in the organization where they work.[25] Indeed, a statistical analysis of technology companies reveals that a longer vesting period for executive stock options is correlated with higher growth rates for the involved business.[26]

A study done at Harvard Business School revealed that stock options encouraged top managers to engage in earnings manipulation, including the reporting of higher discretionary current accruals, larger excess fourth quarter sales, and a greater likelihood of future lawsuits at their firms.[27] So then what incentive system is, in fact, acting as a counterweight, to block top management misrepresentations about the numbers in order to hit a financial target, and to block top management from taking on excessive risk? Certainly being fired or obtaining a bad reputation in the industry are considerations. But this author, after studying the net effects, suggests such counter-incentives are insufficient. Instead, if top management was seriously worried about being sued personally for negligence or recklessness, that should help establish a proper balance. Under the current legal system, however, such a lawsuit rarely occurs.

D. High Straight Level Salaries Reveal Insensitivity to Organization Reputation Problems & Other Related Issues

Top managers are also in many cases paid straight salaries, albeit with very high dollar amounts, as if they were top government bureaucrats.[28] The insensitivity of their pay to public reputation problems, such as those caused by a major information security or privacy breach, is a further incentive to pay less than the necessary level of attention to investment in long-term infrastructure needed to achieve adequate levels of information security and privacy.

---

23. Michael C. Jensen & Kevin J. Murphy, *CEO Incentives—It's Not How Much You Pay But How*, HARV. BUS. REV. 138, 140 (May-June 1990), *available at* https://hbr.org/1990/05/ceo-incentives-its-not-how-much-you-pay-but-how.

24. For a discussion of the perverse impact of externalities on the level of information security infrastructure investment, *see* Lawrence A. Gordon & Martin P. Loeb, *The Economics of Information Security Investment,* 5 TRANSACTIONS ON INFO. AND SYS. SECURITY, 438, 453 (2002); Johannes M. Bauer and Michel J. G. van Eeten, *Cybersecurity: Stakeholder Incentives, Externalities, and Policy Options*, 33 TELECOMM. POL'Y 706 (2009), available at http://dx.doi.org/10.1016/j.telpol.2009.09.001.

25. *See* Charles M. Elson, *What's Wrong with Executive Compensation?,* HARV. BUS. REV. Jan. 2003, at 68, 69, https://hbr.org/2003/01/whats-wrong-with-executive-compensation.

26. Maxwell J. Chambers, *The Effect of Executive Compensation on Firm Performance through the Dot-Com Bubble* (Apr. 23, 2012) (unpublished B.A. thesis, Claremont McKenna College) (on file with Mudd Library, Claremont McKenna College).

27. *See* Joanne Sammer, *Do Incentives Skew Management Priorities*?, BUS. FIN. (Feb. 9, 2012), http://businessfinancemag.com/hr/do-incentives-skew-management-priorities.

28. *See* Jensen & Murphy, *supra* note 23.

The trustworthiness of a firm, and the infrastructure that it has built and uses, is a critical component of not only organizational success, but also organizational viability going forward in time.[29] When a debacle like the Sony hack (mentioned above) takes place, top management generally does not personally pay the price. The corporation is generally thought to be the entity that bears the risk, not members of top management personally. This arrangement, characterized by insensitivity of top management rewards to relevant external conditions, in turn creates incentives for top management to act recklessly.[30] Insufficient investment in the technological infrastructure supporting information security and privacy is just one of the casualties of this reckless behavior.

E. Secrecy Encourages Maintenance of the Status Quo, Even Though Information Systems Technology is Changing the World Dramatically

The exact nature of the employment contract that a top manager has with a commercial firm is generally confidential. The employer wishes to keep such an agreement secret lest it fall into the hands of competitors, and then allow competitors to more easily lure away the involved top manager. The top manager wishes to keep such an agreement secret because revealing it publicly would probably upset other employees of the same organization who did not get such a lucrative deal.[31] In addition, at a particular commercial entity, the executive compensation system and the executive incentive system are likely to be considered proprietary and confidential information, which, in turn, is declared to be restricted information in these employment contracts.[32]

Of course, if these employment agreements are not disclosed to other firms or other employees, they probably are not disclosed to shareholders, customers, unions, or the general public. This lack of transparency prevents these agreements from being challenged because they have embedded conflicts of interest.[33] This lack of transparency also interferes with the duty of shareholders to properly supervise the top managers at the firm in question via the Board of Directors, derivative suits, shareholder activism, and the like. The fact that access to top management compensation related information is a significant issue at all reveals that the existing top management incentive systems are suspect, at the very least.[34]

---

29. *See generally* Marjory S. Blumenthal, *The Politics and Policies of Enhancing Trustworthiness for Information Systems*, 4 COMM. L. & POL'Y 513 (1999).

30. Vikramaditya S. Khanna, *Should the Behavior of Top Management Matter*?, 91 GEO. L.J. 1215, 1215-16 (2003).

31. The current ratio of unskilled worker pay to chief executive pay in the U.S. is now 350:1. Gretchen Gavett, *CEOs Get Paid Too Much, According to Pretty Much Everyone in the World*, HARV. BUS. REV. BLOG NETWORK (Sept. 23, 2014), https://hbr.org/2014/09/ceos-get-paid-too-much-according-to-pretty-much-everyone-in-the-world.

32. Securities & Exchange Commission ("SEC") investor proxy disclosure rules require some executive compensation disclosures, in part to counteract the secrecy that otherwise would surround this information. *See* 17 C.F.R. § 240.14a-101, Item 8 (2014).

33. There is, however, an increased call to make such compensation packages with top managers public. *See* Yonca Ertimur et al., *Shareholder Activism and CEO Pay*, REV. OF FIN. STUD. (Nov. 19, 2010), *available at* http://rfs.oxfordjournals.org/content/early/2010/11/18/rfs.hhq113.full.pdf+html.

34. Jeremy L. Goldstein & Jeremey L. Goldstein & Associates, LLC*, Shareholder Activism and Executive Compensation*, HARVARD LAW SCHOOL FORUM ON CORPORATE GOVERNANCE AND FINANCIAL

Ideally, as a matter of integrity of the structure of the legal and social systems under which we operate, and as a way to foster greater public trust, all such executive compensation arrangements should be made public, and left open to both challenge and periodic revision based on alleged conflicts of interest.

F. Focus on Career Advancement and Personal Fame Leaves Long-Term Investment in Infrastructure in the Dust

One additional employment-market-oriented incentive system that motivates top management is the chance to significantly advance one's career by taking a higher-paying or more prestigious position with another organization. In past decades, many top managers would have been with their company for their entire working careers. Today, frequent job changes are the norm,[35] and along with that higher job change frequency goes the focus on short-term thinking, short-term financial results, and, not surprisingly, an undue acceptance of short-term risks in the information security and privacy areas.

IV. A SHORT HISTORY OF TOP MANAGEMENT PERSONAL LIABILITY FOR INFORMATION SECURITY AND PRIVACY HARMS TO THIRD PARTIES

Limited liability (in the context of business rather than sovereign immunity, diplomatic immunity, parliamentary immunity, judicial immunity, or prosecutorial immunity) was first created in 1844 English law via the corporate form—a separate legal personality. This limited liability was intended to enable endeavors that might not otherwise be possible, such as the financing of a large project like building a network of canals.[36] The legal personality separation of the corporation from the legal personality of individual decision makers, investors, business partners, employees, lenders, and other parties has been and continues to be a hallmark of the corporate organizational structure. As a derivative of English law, the limited liability structure of the modern American corporation combines, and, in multiple ways conflates, the limited liability of investors with limited liability of top decision makers. On a conceptual level, this article claims that superior social welfare results will be obtained if these two types of limited liability are dealt with in a more distinctly separate manner in the law.

In terms of losses caused to third parties resulting from corporate activity, there is convincing economic justification for having corporations bear the risk for unintentional harms in order to encourage both entrepreneurial risk taking and an expanded level of economic activity. But that same justification is not relevant to knowing and intentional harms caused by actions taken by top management. In support of this claim of inapplicability is ample evidence for the "deflection

---

REGULATION (June 18, 2015), https://corpgov.law.harvard.edu/2015/06/18/shareholder-activism-and-executive-compensation.

35. Richard Mills, Hiring Leaders: *A Failsafe Guide to Dominating Any Industry by Employing its Dominant People,* CHALRE ASSOCIATES (2013), http://www.chalre.com/pdfs/Hiring_Leaders.pdf.

36. Paddy Ireland, *Limited Liability, Shareholder Rights and the Problem of Corporate Irresponsibility*, 34 CAMBRIDGE J. OF ECON. 837, 839 (2010), *available at* http://cje.oxfordjournals.org/content/34/5/837.full.pdf+html.

hypothesis" by which top management of corporations has the involved corporation bear a disproportional amount of the risk of knowing and intentional misdeeds for which they are responsible.[37] For example, empirical research shows that when increased directors' and officers' insurance shields top management from personal liability related to mergers and acquisitions, the results are detrimental to shareholder returns.[38]

If corporations are not able to shift some of this risk bearing for intentional and knowing acts back to top management personally, then socially undesirable results are likely to ensue.[39] For purposes of the following discussion about information security and privacy related harms caused to third parties, it is critical that we as a society come to appreciate that inadequate investment in information security and privacy be clearly seen as an intentional and knowing act, an act for which top management should be held personally liable.

At the current time, insufficient top management investment in information security is a vague and often inadequately explored area when it comes to assigning liability for the harms caused to third parties. As will be explained further below, it is now possible to clearly delineate what is an adequate level of investment in information security and privacy, and thus a court can now readily determine whether there has been such an intentional and knowing act on top management's part. Top management personal liability is thus suggested as an appropriate penalty when intentional and knowingly inadequate investment in information security and privacy takes place.

Sanctions imposed on corporations will typically be increased when top management is shown to have been involved through intentional and knowing acts, for example via the "alter ego theory," whereby top management uses the corporation as its own alter ego to pursue personal purposes.[40] Sanctions will also typically be increased if top management can be shown to have directed certain misdeeds, as can be found in the organizational sentencing guidelines found in the Model Penal Code.[41] Of particular concern are those cases where top management takes the corporation down a knowing or reckless path, leading to significant damage to third parties, not just investors, but also customers, prospective customers, business partners, and members of the general public. Recent examples of such knowing or reckless behavior have included firms like Enron, Worldcom, and Global Crossing.

Corporate officers have a variety of duties to their company and to shareholders, including the duty of care, the duty of good faith, the duty of loyalty, the duty of disclosure, the duty of oversight, the duty not to violate the law, and the

37. Khanna, *supra* note 30, at 1254.

38. Chen Lin et al., *Directors' and Officers' Liability Insurance and Acquisition Outcomes*, 102 J. OF FIN. ECON. 507, 507-525 (2011), *available at* http://www.sciencedirect.com/science/article/pii/S0304405X1100184X.

39. Khanna, *supra* note 30, at 1218.

40. For example, the court may pierce the corporate veil and thus hold the owner personally liable, if that the corporate form is a sham (there was actual fraud) and that the corporation was simply acting on behalf of the owner. *See* Latham v. Burgher, 320 S.W.3d 602, 609 (Tex. App. 2010).

41. U.S. SENTENCING GUIDELINES MANUAL § 8C2.5 (2016); MODEL PENAL CODE § 2.07(1)(c) (1985).

duty of reasonable reliance and delegation.[42] Corporate officers may face personal liability if they breach these fiduciary duties, but the standard is quite high, as evidenced by the *Caremark* decision.[43] In general, only the most egregious cases result in either director or officer personal liability. The types of lawsuits now possible for the breach of these duties are either direct or derivate suits and are brought by shareholders or, in some cases, by creditors. There are generally no legally recognized duties of corporate officers to third parties. As discussed later in this article, in addition to other affirmative defenses, there is most prominently the business judgment rule, which generally protects both directors and officers against personal liability.

In the information security and privacy area, there are also several federal statutes that impose responsibility on corporate officers. These include the Sarbanes-Oxley Act, the Gramm-Leach-Bliley Act, and the Healthcare Insurance Portability and Accountability Act. The Federal Trade Commission recently has been quite active in the information security and privacy area acting under authority of the Fair Credit Reporting Act,[44] but the penalties imposed are typically against the involved organization rather than the top managers at that organization.[45] State laws, such as those that dictate how to notify victims of a security breach, may additionally impose some personal liability on top managers.[46] In America, however, there is currently no consistent legal theory or policy regarding top management personal liability for harms caused to third parties.[47] This article suggests the establishment of such a unified legal framework via federal legislation.

To more effectively motivate top management to act in a socially beneficial manner, specifically to invest adequate resources in information security and privacy, the law must consistently hold top management personally liable for harms caused to third parties that ensue from inadequate information security and privacy investment decisions.[48]

V. SUGGESTED WORKING OBJECTIVES THAT WOULD BETTER INCENTIVIZE TOP MANAGEMENT

Turning to the future, and thinking about how the current legal situation could be improved, without delving deeply into the literature of employee incentive

---

42. MATTHEW BENDER, BUSINESS LAW MONOGRAPHS: CYBER SECURITY AND CORPORATE LIABILITY § 1.02 (4th ed. 2015).

43. *See* In re Caremark Int'l Derivative Litig., 698 A.2d 959 (Del. Ch. Ct. 1996).

44. BENDER, *supra* note 42, at § 2.03.

45. *See*, e.g., Complaint ¶6, Eli Lilly Co., No. C-4047, (FTC May 8, 2002), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2002/05/elilillycmp.htm (alleging the company, not top managers, violated the privacy of persons who had signed up for email reminders to take certain medications).

46. *See*, *e.g.*, CAL. CIVIL CODE §§ 1798.29 and 1798.82 (West 2016).

47. BENDER, *supra* note 42, at § 2.03(5)(a).

48. Others, in addition to this author, suggest the employment of negligence as a motivator to get management to act in a manner to reduce information security and privacy-related losses. Consider proposals to employ negligence in order to force software vendors to incorporate more security and privacy in their products, as discussed in Michael L. Rustad & Thomas H. Koenig, *The Tort of Negligent Enablement of CyberCrime*, 20 BERKELEY TECH. L.J. 1553, 1557 (2005).

system design, we can generally posit ten desirable attributes for an incentive system.[49] These ten general attributes for a successful incentive system are:

(1) Explicitly stated objective criteria that are easily measurable and ideally quantitative,

(2) Criteria based on feedback coming from disinterested sources such as non-conflicted third parties or other sources that are not subject to manipulation (low distortion potential),

(3) Criteria reflective of a significant range of behaviors over which the measured employee has control so as to directly affect the results,

(4) Criteria perceived as significantly impactful on employee rewards and/or penalties,[50]

(5) Criteria consistent with other motivational forces such as promotions and the threat of termination,

(6) Criteria unlikely to be distorted by factors uncontrollable by the employee,

(7) Criteria unlikely to produce employee behaviors that are problematic or dysfunctional to the organization,

(8) Criteria consistent with the employer's strategic values and priorities,

(9) Criteria reliant on skills and knowledge possessed by, or readily acquired by, the employee, and

(10) Criteria simple to understand and reasonably inexpensive to apply.

The proposed draft law, which is expressly laid out in the appendix to this article, looks particularly attractive in light of these ten incentive system design attributes. Responding to each of the ten design criteria set forth above, this draft proposed law would:

(1) Employ objective criteria that are both readily measurable and objective, criteria indicating whether top management has acted in a manner that is in keeping with an expanded definition of the duty of due care, and criteria that addresses whether top management has employed a safe harbor provision to ensure the organization would be adequately protected.

(2) The law would be based on feedback coming from non-conflicted disinterested third party auditors or expert consultants—people who are not under the direct or indirect control of top management.

(3) The extent to which top management may be liable or culpable under the new law is directly linked to top management's performance in this important area of information security and privacy.

(4) The new law is furthermore likely to be a significant motivator to spur top management to act in a more responsible and forward-thinking manner. Through compliance, top management will avoid the unnecessary exposure of their personal assets to the liability established by the law. In addition, because the law helps to maintain the good reputation of top managers in a community, the law has

49. *See generally* Michael J. Gibbs, et al., *Performance Measure Properties and Incentive System Design*, 48 INDUS. REL. 237 (2009).

50. *See generally* Sindri Thor Hilmarsson & Pall Rikhardsson, *The Evolution of Motivation and Incentive Systems Research: A Literature Review*, *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1965646.

psychological and reputational benefits as well.

(5) The proposed law also appears to be consistent with most common types of corporate incentive systems, such as performance review systems, and thus appears able to readily become a significant component of a set of incentives that cause top management to act in socially responsible ways.

Furthermore, indicating the topics to be addressed in the balance of this article, it is readily observable that:

(6) The proposed law directly addresses the long-term dynamic experience of a particular organization in the information security and privacy area, rather than external factors such as a normative static model of good security and privacy, and is thus most unlikely to be distorted by extraneous factors outside the control of top management.

(7) Since it affects the personal, financial, and reputational status of top management, the proposed law is additionally likely to produce the intended effects, notably an improvement in the experienced level of information security and privacy. Furthermore, since the new law encourages the provision of a stable and reliable information systems infrastructure in support of other organizational goals and objectives, the law helps foster congruence and alignment among organizational activities.

(8) The proposed law is unquestionably consistent with organizational goals such as fostering good customer relations, being a reliable business partner, avoiding the distraction and cost of unnecessary litigation, and maintaining a good public reputation.

(9) The new law addresses results that are directly under the control of top management, for example the top managers can decide to retain expert consultants necessary to provide them with safe harbor protection against lawsuits.

(10) The structure of the proposed law is relatively simple, and both its impact and its implications can readily be understood by interested constituencies, such as top management, employees implementing the law, customers, business partners, and the general public.

It is the top executive in charge of setting and approving the budget for information security and privacy that should be held primarily liable for information security and privacy. This is consistent with a recent New York Stock Exchange Survey,[51] which noted that the boards of directors hold Chief Executive Officers primarily responsible for security and privacy problems. They hold the Chief Information Officer secondarily responsible. In keeping with standard industry practice, which this author suggests is a reflection of where the true power, responsibility, and accountability lies, this article focuses on the liability of the top manager who establishes and approves the budget for information security and privacy within the organization.

---

51. *See generally* Robert Hackett, *Here's Who [sic] Boardrooms Are Blaming for Data Breaches*, FORTUNE (May 29, 2015, 10:18 AM), http://fortune.com/2015/05/29/boardroom-data-breach-blame.

VI. WHY WE MUST NOW EXPRESSLY DEFINE A DUTY OF CARE FOR THE NEW STEWARDS OF THE PUBLIC TRUST

A. The Public Demands Greater Top Management Responsibility Toward the Larger Community

There is widespread acknowledgement in the information systems management community that the law regarding information security and privacy needs to be changed.[52] The law notably needs to be coordinated and centralized at the federal level to bring standardization and rationalization to what is often a patchwork of state laws.[53] Recent efforts to change the law have focused on better sharing of information between interested parties.[54] Many recently proposed laws have also focused on identifying, pursuing, and punishing the perpetrators.[55] A focus on increasing penalties for perpetrators of computer crimes is illogical if one understands the economics of prisons; far more money must be spent on confining prisoners than is required for a single prisoner to break the systems that imprison him.[56] The same economic relationship holds true for information security and privacy, and the focus should thus be on the protectors, not on those who break existing protection mechanisms. Thus the focus of new and improved law must instead be on motivating top management at target organizations to better protect their systems.

Unfortunately to date, very few parties have publicly discussed the dysfunctional management incentive systems that have markedly contributed to this current state of emergency—the incentive systems that are directly addressed in this article. As an indication of the urgent need to bring greater seriousness to the information security and privacy area, consider that the European Union's new privacy regulations can involve the imposition of a fine of up to 4% of a corporation's global revenue.[57] The potential downside risk of inadequate information security is thus rapidly increasing in order to get top management's attention and to motivate top management's constructive action. The Europeans are leading the way in terms of using financial incentives to gain the attention of top

52. Noah G. Susskind*, Cybersecurity Compliance and Risk Management Strategies: What Directors, Officers, and Managers Need to Know*, 11 N.Y.U. J.L. & BUS. 573, 582 (2015).

53. Randy Sabett, *Another Call for Federal Data Privacy Laws*, TECH TARGET NETWORK (May 2014), http://searchsecurity.techtarget.com/feature/Breach-patrol-Another-call-for-federal-data-privacy-laws.

54. Hunton & Williams, *U.S. Congress Releases Compromise Bill on Cybersecurity Information Sharing,* PRIVACY & INFO. SECURITY L. BLOG (Dec. 17, 2015), https://www.huntonprivacyblog.com/2015/12/17/u-s-congress-releases-compromise-bill-on-cybersecurity-information-sharing.

55. *See generally* Steven Robinson, *U.S. Information Security Law, Part 3*, SYMANTEC, (May 11, 2003), http://www.symantec.com/connect/articles/us-information-security-law-part-3.

56. Sometimes called the "jailer's dilemma," this concept is based on the economics of incarceration, which reveals that considerably more resources must be employed to keep a prisoner incarcerated, than are needed to break out of a jail. The same is true in information security and privacy, namely that far more resources must be spent to avoid, prevent, detect, deter, correct, and recover from problems than are required to compromise the controls established to prevent such problems.

57. *See generally* Cyrus Farivar, *Tech Firms Could Owe Up to 4% of Blobal Revenue If They Violate EU Data Law*, ARS TECHNICA (Dec. 15, 2015), http://arstechnica.com/tech-policy/2015/12/tech-firms-could-owe-up-to-4-of-global-revenue-if-they-violate-new-eu-data-law.

management.

The public is very much aware that there is a lack of alignment between the personal objectives of top management and the objectives of third parties, such as customers.[58] Consider an article by former Goldman Sachs executive director, who recently stunned the Wall Street community when he left his job. He explained why he left saying, "[t]o put the problem in its simplest terms, the interests of the client continue to be sidelined in the way the firm operates and thinks about making money."[59] What is needed now is not further polarization between the rich and powerful, such as top management, on one hand, and the rest of society on the other hand. What we need is an alignment of objectives, so that top management is forced to act in a manner that is consistent with the interests of the larger society, rather than simply in favor of their own interests, or alternatively, in favor of their own interests plus those of shareholders. The real question is not so much about human nature and whether people act in their own interests, as it is about how we can find alignment[60] so that what is best for various constituencies such as business partners, customers, and the general public is also best for the top managers choosing those options.[61]

According to one survey involving 33,000 respondent adults with college educations, some 81% agree that a "company can take specific actions that both increase profits and improve economic and social conditions in the community where it operates."[62] That same study noted the reasons that trust in business has decreased in recent times. One of these reasons, noted by some 53% of the respondents, was that business "failed to contribute to the greater good."[63] The conversation in this area is unfortunately often polarized into a duality, and many people erroneously believe we must have either management doing a good job for the company and investors, or management attending to community concerns such as environmental pollution and information security and privacy. To assure the stability and sustainability of our economic and political systems, top management can and must simultaneously serve all of these objectives.

In the area of top management's obligation to third parties, not just to the corporation and shareholders, there has been some significant recent change. For example, some thirty states now permit or require directors to consider the effect of their decisions not just on shareholders, but on employees, suppliers, customers,

---

58. Even international business magazines readily admit this fact. See *Editorial, Reinventing the Company*, THE ECONOMIST (Oct. 24, 2015), *available at* http://www.economist.com/news/leaders/21676767-entrepreneurs-are-redesigning-basic-building-block-capitalism-reinventing-company ("[A]fter a century of utter dominance, the public company is showing signs of wear. One reason is that managers tend to put their own interests first.").

59. Greg Smith, *Why I Am Leaving Goldman Sachs*, N.Y. TIMES, (Mar. 14, 2012), http://www.nytimes.com/2012/03/14/opinion/why-i-am-leaving-goldman-sachs.html.

60. This discovery of a place in the law where there is alignment of incentives is also seen in the arena of climate change. *See*, *e.g.*, Elizabeth Burleson, *From Coase to Collaborative Property Decision-Making: Green Economy Innovation,* 14 TUL. J. TECH. & INTELL. PROP. 1 (2011).

61. *See generally* Korn Ferry Institute, *Selfish or Self-Interest?,* BRIEFINGS MAG. (May 11, 2012), available at http://www.kornferry.com/institute/424-selfish-or-self-interest.

62. Kathryn Beiser*, A New "Business as Usual,"* EDELMAN (Jan. 19, 2015), http://www.edelman.com/post/a-new-business-as-usual/.

63. *Id.*

creditors of the corporation, and local communities.[64] One example of the trend toward considering the interests of other constituencies besides the corporation and its stockholders comes from Pennsylvania, and that state's law not only permits directors to consider the interests of the other parties, but it also expressly encourages a long-term time horizon rather than simply short-term financial gain.[65]

B. Information Systems Technology Has Changed Dramatically, Especially With the Internet

Today, the attack launching points have expanded to include a host of mobile devices such as tablets and smart phones, and those launching points can be located anywhere in the world. Using widely available scripted attack software, non-technical criminals from other countries– countries with which the United States has no extradition treaties– can launch attacks to drain off American financial assets. In the past, in-person attacks, such as robbing a bank with a gun, were necessary. Accordingly, the job of information security and privacy today is vastly more difficult (for example, using encryption, hashing, and digital signatures for files) than it was in the past (for example, using locking file cabinets), and thus the old-fashioned approaches to management will no longer suffice. The job is furthermore considerably more complex because so many of the critical assets that must be guarded are intellectual property assets such as copyrights, patents, and trademarks.[66] Therefore, top management must step up to a much more dedicated, professional, and orchestrated effort in the information security and privacy area.

The targets that are reachable via the Internet are also much more varied and available than they used to be. Now, thanks to the "Internet of Things," we have refrigerators, burglar alarm systems, natural gas leak detectors, and a wide variety of other types of equipment,[67] including large industrial plants like oil refineries, as targets that are Internet-connected and potentially vulnerable to attack. The adverse implications of deficient management of information security and privacy are grave and worthy of the most serious consideration of Congress as well as worthy of significant new legislation that is promptly enacted.

Our economy has become incredibly dependent on reliable, readily available, and ubiquitous information. For example, health care records are exchanged between doctor's offices, clinics, hospitals, and insurance companies. If that patient health care information were to be altered by unauthorized parties, great harm (such as prescribing the wrong drugs) could be done. Identity theft provides another example of how the lives of Americans are largely governed by information,

64. Anthony Page, *Has Corporate Law Failed? Addressing Proposals for Reform*, 107 MICH. L. REV. 979, 988 (2009).

65. 15 PA. CONS. STAT. ANN. § 1715(a)(1) (2013).

66. PRICEWATERHOUSECOOPERS, GLOBAL STATE OF INFORMATION SECURITY SURVEY 2017 (2016), *available at* http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html (indicating that theft of intellectual property increased 56% over the prior year).

67. Catalin Cimpanu, *Script Kiddies Can No Launch XSS Attacks Against IoT Wind Turbines*, SOFTPEDIA (Dec. 8, 2015, 10:30 PM), http://news.softpedia.com/news/script-kiddies-can-now-launch-xss-attacks-against-iot-wind-turbines-497331.shtml (describing remote attacks on wind turbines and how hackers can make them less efficient).

information that must be readily available, must be correct, and also must be kept securely and privately. The functioning of our modern American economic system now depends on the reliable handling of such information, and if top management has not been addressing security and privacy adequately, it can hurt many more groups of people than simply the donors, stockholders, taxpayers, or other primary constituency at the organization where top management works.

Our tightly integrated information-based economy is also increasingly vulnerable to unavailability of the information on which it depends. If, for example, the major stock markets, commodity markets, and/or bond markets, all of which are highly-automated, were to be tampered with, a host of related businesses in the financial services sector would suffer severe losses, and perhaps even be unable to operate for a period of time due to a systemic loss of trust in the systems on which these firms rely. This very tight integration means that top management cannot simply look to the corporation and its shareholders (or its equivalent in other organization types) when making decisions; top management must also look to third party stakeholders when making decisions related to information security and privacy.

C. Business Structures and Relationships Have Changed Dramatically, Especially With Globalization and Outsourcing

In the past, business activities proceeded in a much more separate and isolated manner. Hundreds of years ago, a sole proprietor with a factory making hats might personally direct a handful of employees. Their activities were largely separate from other parts of the economy, for example because each employee performed many different tasks that today would be assigned to many different specialists. Back then, employees were effectively "servants," to use the old legal term, and it was appropriate for their sole legal duty and loyalty to be owed to their employer, then called the "master". Today, information is being exchanged much more extensively, for example, through social networks like LinkedIn™, so people are not nearly as isolated as they were back then. Business networks of relationships are much more extensive and enmeshed now, the number of parties involved in a process such as making hats is much greater, and the degree of specialization that each party plays is also much greater. Thus today, people are coming together more intimately, they are communicating with each other more extensively, and they are reliant on each other in unprecedented ways. All this means that we are all engaged in networks of multi-organizational business relationships, and for the law to recognize only one set of duties for top management, namely to the corporation (and by extension to the shareholders), that exclusive focus creates dangerous and distorted effects, such as serious vulnerabilities in the information security and privacy area.

The Internet has facilitated the spread of global business, increased the level of competition, and accelerated the pace of business activities. At the same time, it has introduced a wide variety of legal inconsistencies, and created new questions, including questions to which there are presently no clear answers. How, for

example, is a multinational corporation going to consistently handle the inconsistencies in privacy regulations across countries?[68] And by which involved country should a multinational criminal gang operating on the Internet be investigated?[69] The provision of goods and services via the Internet from many different countries has also jeopardized both national and state sovereignty, for example, making it unclear whether sales taxes must be collected on certain transactions handled via the Internet.[70] For American business to remain competitive in this new Internet-based business environment, top management cannot simply passively wait until these and related matters are resolved. Their attention to these and related issues, including information security and privacy, is urgently needed. But unless top management is strongly motivated to take these issues seriously, they will continue to employ a laissez-faire approach, in many cases simply waiting for the dust to settle before taking decisive action.

Without getting too technical, it is important to highlight one aspect of the increased tempo with which the Internet now forces business to operate. In the past, a responsive and reactionary manual approach to attacks was sufficient. For example, if a string of banks were to be robbed by a gang driving a car through the southern U.S. states, such as the Bonnie and Clyde gang in the 1930s, then a local police posse would be sent out to apprehend them. But responsive and reactionary approaches alone are totally insufficient in the age of Internet-based crime, Internet-based terrorism, and Internet-based cyber war. Having only a manual-based reactive response to meet an automated attack is a recipe for serious losses. This is because many attacks are now automated, and that fact means that defensive measures must similarly be proactive, scripted, and automated.[71] But very few organizations have automated scripted defensive maneuvers implemented to protect their Internet-connected information systems. A whole different level of sophisticated defense[72] urgently needs to be developed and implemented, and top management must be motivated to pay for and oversee the development of such sophisticated defense systems. This author submits that top management will not be so motivated unless the legal incentive system to which they are subject is altered as described in this article.

---

68. *See generally* Angela Vitale, *The EU Privacy Directive and the Resulting Safe Harbor: the Negative Effects on U.S. Legislation Concerning Privacy on the Internet*, 35 VAND. J. TRANSNAT'L L. 321 (2002).

69. *See generally* Robert M. Pitler, *Independent State Search and Seizure Constitutionalism: The New York State Court of Appeals' Quest for Principled Decisionmaking* [sic], 62 BROOKLYN L. REV. 1 (1996).

70. *See generally* Douglas Huenick, *Comment, Eliminating the E-Commerce Sales Tax Advantage in the United States by Following in the Footsteps of the European Union*, 31 WIS. INT'L L.J. 65 (2013).

71. *See* Richard Steinberger, *Proactive vs. Reactive Security*, EN POINTE BLOG (June 30, 2014), http://www.crime-research.org/library/Richard.html.

72. Alexander Pretschner et al., *Raising the Bar for Automated Attacks Against Web Applications Using Software Diversity*, (unpublished Master's thesis, Technische Universität München) (on file with Technische Universität München), *available at* https://www22.in.tum.de/fileadmin/w00bwn/www/thesis_proposals/Raising_the_Bar_for_Automated_Attacks_against_Web_Applications_using_Software_Diversity.pdf (describing research now underway indicative of the type of scripted defensive work that needs to be done).

D. The Rights of Third Parties Are More Directly and Profoundly Affected by Top Management Decisions

i. New Interconnectivity Brings New Relationships

The new interconnectivity that the Internet, cell phones, and modern computer-related technology has brought, when combined with modern business arrangements, requires that top management exercise a new level of responsibility, diligence, and care and concern for parties other than the corporation and by extension its stockholders. For example, when a business gathers personal information about customers, and maintains that same information in its computer systems, it should have a duty to the customers to prevent that information from falling into the wrong hands.[73] The customers are reliant on top management at the business involved to adequately protect the security and privacy of their information. For management to fail to use reasonable care in the protection of this personal information is akin to the tort of negligent undertaking.[74] That tort involves the imposition of a legal duty, where a duty would not otherwise exist, because third parties relied upon the perpetrator to offer a safe product or service. This same tort was, for example, used in litigation related to breast implants.[75]

The notion of a duty to third parties[76] can also be seen in the creation of a neighborhood hazard (legally speaking, an "attractive nuisance"[77]) such as a swimming pool. Unless a locked fence is placed around the pool, the pool is adequately maintained, and the pool is properly supervised when used, the pool owner may be held liable for injuries sustained.[78] Similarly, top management at organizations, whether non-profit, for-profit, or governmental, uses a shared resource called the Internet, and is also the custodian of customer information, so third party customers rely upon top management to do the right thing with respect to their personal information.[79]

---

73. *See*, e.g., Palsgraf v. Long Is. R.R. Co., 162 N.E. 99 (N.Y. 1928) (illustrating the absence of a duty to third parties such as customers). In that case, the court ruled that the railroad had no duty to protect a bystander who was injured from threats that are not immediately obvious to the railroad's employee. But such an approach is out of place in the modern world of information security and privacy, where there are many threats that are not immediately obvious, such as computer viruses, and top management should therefore be held responsible for protecting against such threats.

74. RESTATEMENT (SECOND) OF TORTS § 324A (AM. LAW INST. 1965).

75. In re Silicone Breast Implants Prods. Liab. Litig., 887 F. Supp. 1447 (N.D. Ala. 1995).

76. The type of duty to third parties recognized in the draft law provided in this article is consistent with existing negligence statutes, such as negligent infliction of emotional distress in California. The latter claim can only be brought in three limited circumstances: (1) negligent handling of a corpse, (2) negligent misdiagnosis of a disease that could potentially harm another, and (3) negligent breach of a duty arising out of a preexisting relationship. It is the nature of this third possibility, a preexisting relationship, which is redefined and broadened in the draft law. Burgess v. Superior Court, 831 P.2d 1197 (Cal. 1992).

77. RESTATEMENT (SECOND) TORTS § 339 (AM. LAW INST. 1965).

78. Botner v. Bismarck Parks and Recreation Dist., 782 N.W.2d 662, 663 (N.D. 2010) (finding that the owner of a pool may be held liable for injuries suffered under improper supervision).

79. The law now creates inequitable results because no duty of management is recognized toward third parties. *See*, e.g., Huggins v. Citibank, 585 S.E.2d 275, 277 (S.C. 2003). In this case, a victim of identity theft attempted to hold a bank responsible for negligently issuing credit cards in his name. Id. The banks issued credit cards without any investigation, verification, or corroboration of the applicant's identity, yet the court said there was no duty to the plaintiff victim of identity theft because he was not a customer of the banks. Id.

Not only are third parties now inescapably reliant on top management at organizations to responsibly manage information security and privacy, but the consequences of top management's failure to adequately and responsibly manage this crucial area are potentially much more damaging than in decades gone past. For example, Internet access to computerized control systems[80] can allow, and, in fact, demonstrably has already[81] allowed, a remote attacker to shut down the electrical power grid for a large geographical area. Thus, these new relationships, the ones that information systems and networking technology enable, bring a significant magnification of the scale of the damage that might be sustained by third parties due to inadequate information security and privacy.

ii. Recognition of Rights of Third Parties Increasingly Found Elsewhere in the Law

Likewise, there are some circumstances in which the rights of third parties should be recognized and management should not solely be accountable to the corporation (and by extension to the shareholders thereof). Consider a case of insolvency, where there has been a breach of duty by the management at the firm, and as a result, the creditors have lost their money.[82] While the duty of the management may not normally extend beyond the shareholders, if management's breach of duties was the cause of the loss, then management should be held accountable to the creditors, and not permitted to simply shift the loss to the shareholders. Coming back to information security and privacy, if management has breached its duty to third parties, it should be held personally responsible, and likewise, it should not be able to simply transfer the risk to shareholders.

iii. Increasingly Mandated Terms of Social Engagement

There are other situations in which reliance on top management can be used to create a duty to third parties. This is particularly true when the third parties have no choice but to rely on top management to protect their personal information. Many aspects of modern business have characteristics of "contracts of adhesion," in that the customer has only two choices: (1) accept the standardized terms and conditions that the business offers, because the product or service is desired, or (2) do not accept those terms and conditions, and forgo the product or service. Many of these products and services are necessary for ordinary life, for instance a credit or debit card is generally necessary to buy an airplane ticket on the Internet. If the terms of

80. Technically, such systems are called Supervisory Control and Data Acquisition (SCADA) systems. Many industrial infrastructure control systems, such as those that control electrical power transmissions, oil and gas pipelines, and chemical plant manufacturing operations, are controlled via SCADA systems. For an overview of the possible information security and privacy attacks against modern SCADA systems, *see* BONNIE ZHU ET AL., A TAXONOMY OF ATTACKS ON SCADA SYSTEMS (2011), http://bnrg.cs.berkeley.edu/~adj/publications/paper-files/ZhuJosephSastry_SCADA_Attack_Taxonomy_FinalV.pdf.

81. L. Todd Wood, *Ukraine: Russia Hacks Power Plants, Highlights U.S. Weakness*, THE WASHINGTON TIMES (Dec. 30, 2015), http://www.washingtontimes.com/news/2015/dec/30/l-todd-wood-ukraine-russia-hacking-power-plants-hi/.

82. This scenario follows closely with the facts in Francis v. United Jersey Bank, 432 A.2d 814, 817 (N.J. 1981).

such an adhesion contract are unconscionable, fraudulent, or contrary to public policy, then they can be modified or disregarded.[83] If, for example, a mandated arbitration clause would be clearly detrimental to the customer, because it would deny the customer his rights, then it may be set aside by a court of law. This is justified under the notion that many customers do not read such contracts, and even if they did read the contracts, in many cases they could not understand the legal terms therein. Actual assent on the part of consumers in such circumstances is a legal fiction.[84] Similarly, the current information security and privacy arrangements that third parties make with top management is not the result of a fair bargain struck between parties on a level playing field, because the third party customers are not privy to relevant information security and privacy information. Since these modern arrangements do not protect the interests of third parties, nor do they recognize that a duty to third parties exists, they must now be set aside, as further described below in this article. To fail to recognize a top management duty to third parties is now itself unconscionable.

iv. Third Parties Detrimentally Rely on Management to Look After Their Interests

This same argument for a top management duty of care owed to third parties, for damage done due to negligent or reckless management of information security and/or privacy, can be approached from the standpoint of "equitable estoppel" (also referred to as, "estoppel in pais"). Equitable estoppel[85] would bar a party, in this case top management, from asserting a legal claim or defense because that would be inconsistent with his or her prior action or conduct. Generally equitable estoppel prevents one party from being harmed by another's voluntary conduct.

In this case, customers did business with an organization and, by implication, also with top management at that organization. In such a case, top management also, either implicitly or explicitly, represented that they would protect the customer's personal information as part of the transaction. Later, an attack may have leaked such personal information to criminal third parties so that identity theft, privacy invasion, and other harms were possible. To hold top management responsible for the loss would be possible, under the doctrine of equitable estoppel, because there had originally been some detrimental reliance that had induced the customer to do business with the firm in question. Here, the use of equitable estoppel to recognize a duty to third parties would not so much create a right, as it would deny top management the ability to use certain defenses that would block third party claims for damages. These defenses include the agency relationship, the business judgment rule, and the assumption of risk, all of which are taken up in greater detail below.

83. *See generally* Bayes v. Merle's Metro Builders/Blvd. Contr., No. 2007-L-067 (Ohio Ct. App. 2007).

84. Alan M. White & Cathy Lesser Mansfield, *Literacy and Contract*, 13 STAN. L. & POL'Y REV. 233, 242 (2002).

85. RESTATEMENT (SECOND) OF CONTRACTS § 90 (AM. LAW INST. 1981).

E. A Standard of Due Care Now Must Include Duties to Third Parties, Not Just the Duty to an Employer via a Fiduciary Relationship

Economists have long discussed the "tragedy of the commons," where every individual tries to reap the greatest personal benefit from a shared resource.[86] For example, in the early days of colonization of America, if a plot of land were set aside for the grazing of cattle, too many cattle could be placed on the land so that the land would be denuded and the soil then eroded. Then the resource would become markedly less valuable to anyone. This happens because demand overwhelms supply, and every individual who continues to consume what is in the commons then harms others who cannot any longer enjoy the benefits of the shared resource.

The Internet is a shared resource with similar attributes to this hypothetical plot of land. If top management has failed to allocate sufficient resources for security and privacy, they may enjoy higher than otherwise obtainable short-term benefits like a bonus based on high firm profits. But others will suffer as a result, and everyone will be poorer if this state of affairs is permitted to continue. In order to stop the overconsumption of the shared resource, responsibility for managing that resource must be established. The assignment of responsibility to top management, to observe a duty of care to third parties for information security and privacy, achieves that end. This type of solution, where responsibility for protection of a shared resource is fixed and assigned, has worked reasonably well for Antarctica, which is protected by a treaty that specifies that the continent will not be developed for its natural resources and will not be militarized.[87]

One of the significant problems in many prior legislative efforts to improve information security and privacy was that they have expressly specified controls, management solutions, technologies, or other fixed mechanisms that will, especially with the rapid speed of change in the information systems field, soon become obsolete. What instead must be defined is a reference point with which the duty of care for top management can be specifically determined. The proposed law in this article does that by making reference to a standard of due care for a particular industry. Furthermore, the standard of due care is recognized as a dynamic group of controls that will, like the common law, change over time. No attempt is made to specify in the law, or even via implementing regulations, exactly what control or solutions must be used by a certain organization in order to achieve an acceptable level of information security or privacy. This flexible approach helps to assure that the law stays relevant and speaks directly to the way to determine and measure compliance with a standard of due care, that is specific to a particular industry, at a particular point in time.

Note that only a duty of care toward third parties is needed.[88] It is not necessary

86. Many attribute the coinage of this term to Victorian economist William Forster Lloyd. It denotes a situation where individuals acting independently and rationally according to their own self-interests behave in a manner that is contrary to the best interests of the collective because some common resource is thereby depleted.

87. The Antarctica Treaty, Dec. 1, 1959, 12 U.S.T. 794, 402 U.N.T.S. 71.

88. Scott J. Shackelford et al*., Toward a Global Cybersecurity Standard of Care?: Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International*

to recognize a fiduciary relationship from top management to third parties. The only fiduciary relationship that top management now has is with the corporation itself (via the board, and ultimately the shareholders). There is no attempt to change that arrangement in this proposed law, and so all the existing law about fiduciary relationships for top management would remain the same if this proposed law were to be adopted. A fiduciary relationship holds that the agent has a duty to act for the principal's benefit in all matters connected with the agency relationship.[89] A new fiduciary relationship with third parties would be onerous for top management, when all that is needed is a formal legal recognition that a person of ordinary prudence would have exercised care under the circumstances, so that negligence and recklessness (both in the civil and criminal domains),[90] and the damages that go along with negligence and recklessness (such as punitive damages), can then be established without certain affirmative defenses unduly blocking this process. This same least disruptive approach has been adopted in the law at the end of this article.

F. Differential Power of Negotiating Parties Mandates Greater Top Management Personal Responsibility

i. When Such Great Power is Held in the Hands of Top Management, It Requires Greater Accountability

Top managers must now be legally recognized as stewards of the public trust,[91] because they call the shots related to the management of information systems and network infrastructure on which all industrialized nation societies now depend. Top management is the only group making decisions about information security and privacy—decisions that can adversely affect millions, even billions, of people.[92] Top management is making these decisions without any public visibility or accountability, unless of course there is some legal action resulting from the ensuing major losses.[93] The impact of these decisions can range from permitting an

---

Cybersecurity Practices, 50 TEX. INT'L L.J. 305, 314 (2015).

89. RESTATEMENT (THIRD) OF AGENCY § 8.01 (AM. LAW INST. 2006).

90. RESTATEMENT (THIRD) OF TORTS LIABILITY FOR PHYSICAL & EMOTIONAL HARM § 3 (AM. LAW INST. 2006); RESTATEMENT (SECOND) OF TORTS § 282 (AM. LAW INST. 1965).

91. Some more recent cases indicate that the courts realize that top management is often the only one who is, in fact, able to make the changes that are necessary. In Kline v. 1500 Mass. Ave. Apt. Corp., 439 F.2d 477 (D.C. Cir. 1970), the court held that a landlord was under a duty to take precautions for the safety of tenants "as are within his power and capacity to take" in order to prevent criminal intrusion into the building. Id. at 487. In that case, no tenant had the power to take these precautions, such as setting up a CCTV system to monitor the hallways. Id

92. Consider that hackers caused a power grid blackout affecting a large part of the Ukraine in October 2015. Alex Hern, *Ukrainian Blackout Caused by Hackers that Attacked Media Company, Researchers Say*, THE GUARDIAN (Jan. 7, 2016), *available at* http://www.theguardian.com/technology/2016/jan/07/ukrainian-blackout-hackers-attacked-media-company.

93. For example, in the Sony Pictures hack mentioned earlier in this article, emails exchanged between top management at Sony and the U.S. State Department were revealed. These emails discuss propaganda, the national security implications, and the potential fallout of releasing the movie called "The Interview." *See* William Boot, *Exclusive: Sony Emails Say State Department Blessed Kim Jong-Un Assassination in "The Interview,"* THE DAILY BEAST, (Dec. 17, 2014; 2:30 AM), http://www.thedailybeast.com/articles/2014/12/17/exclusive-sony-emails-allege-u-s-govt-official-ok-d-controversial-ending-to-the-interview.html.

error that seriously pollutes a public water supply, to enabling the unauthorized shut down of a nuclear power plant, to permitting an industrial spy to steal valuable intellectual property on which a business' competitive position has been built.[94]

What is now at stake in the information security and privacy field is so potentially significant, widely felt, and impactful, it is not sufficient to allow top management to make these decisions on their own without being subject to serious and quite impactful repercussions if they do not properly safeguard the public trust. The draft law at the end of this article attempts to define the circumstances in which these repercussions might be felt by top managers who did not live up to their duty of care to the public and specific third parties.

ii. Decision-Making Information—Such as Trade-Offs Between Competing Objectives—Is Known Only by Top Management

Since top management alone is calling the shots, they are making critical decisions about information security and privacy—decisions that often nobody knows about except those who work for the organization and report directly to these top managers and, of course, the involved internal and external auditors.[95] The opaqueness of and secrecy associated with such decision-making can be justified under the legitimate claim that if such information were to fall into the hands of third parties, then it could be used to compromise the security and privacy of the systems at the organization in question.[96] But since third parties, like business partners, customers, news reporters, and the general public are not privy to the information security and privacy decisions that top management makes, these and other third parties cannot possibly negotiate in an informed manner or on an equal playing field, on matters related to information security and privacy. The only choice that third parties have is the equivalent of an adhesion contract—effectively a "take it or leave it" deal. Thus, if an adequate level of information security and privacy is going to be obtained, that adequate level must be measured and gauged by what was created as a result.

With this secrecy and opaqueness kept in mind, we can conclude that if serious losses were sustained because top managers did not adhere to their duty of care with respect to third parties, then those top managers should be held personally liable. On the other hand, if no serious losses were sustained, we can infer that, at least for

---

94. Things are getting much worse as well. According to one highly respected annual survey of business, 2015 saw 38% more detected information security incidents than the prior year, and the detected incidents of intellectual property theft increased 56% in 2015 as well. PRICEWATERHOUSECOOPERS, *supra* note 65, at 24.

95. Freedom of Information Act limitations for proprietary information, trade secret laws, sealed court records, confidential settlement agreements, and confidentiality provisions found in contracts will often block information about these security and privacy decisions from being discovered by the general public, interested third parties, or the media. Note that this Act relates to the federal government only. *See* 5 U.S.C. § 552 (2016).

96. While "security through obscurity" is generally not a desirable strategy because auditors and experts should examine controls to determine whether they are working properly, there is definitely a place for keeping security and privacy information confidential. The way that the proposed law in the appendix to this article deals with the need for "another pair of eyes" is through expert third party audits. There is no call for, nor is there a need for, disclosure of control information to the general public, customers, shareholders, or other large groups of people.

the time being, top management's duty of care to third parties appears to have been met. Of course, due to the opaqueness and secrecy of the relationship between top management and third parties and the associated lack of third party knowledge about what actually goes on behind the scenes, the duty of care may not, in fact, have been met. If the liability exposure described in this article's proposed law, however, is adopted, management will nonetheless be spurred to do the right thing because there will be a prospect in the near future that serious losses may be suffered, at which point top management could be held personally liable for those losses.

iii. Third Parties Lack Legal Property Rights in Their Own Information with Which to Gain Negotiation Leverage

On a related point, the law also puts third parties at a distinct power disadvantage in this negotiation with top management about information security and privacy because information about third parties is not recognized as the property of those same third parties.[97] Thus, it is, for example, the sole decision of top management to keep or delete certain personal information which may be innocuous and seemingly insignificant, but later, when new data mining systems are employed, may help to paint a picture about personal activities that would reveal information that the third party never intended to reveal (thereby disclosing medical conditions, sexual orientation, political leanings, etc.).[98]

Third parties are forced to disclose personal information in order to get desired products and/or services that the organization in question is providing. Third parties, such as consumers buying software, do not really have any bargaining power when it comes to how information about them will be stored, protected, shared, etc.[99] While there are some basic laws about disclosure and limited sharing of personal information in some industries such as banking[100] and health care,[101]

---

97. This is distinctly different than member states in the European Union, which do recognize third party rights in information that describes them. See Council Directive 95/46/EC, art. 1, 1995 O.J. (L 281) 38. This right is more recently in the news because the European Union recognizes the right of individuals to have no-longer-occurring personal information about them removed from public records. This is more colloquially known as the "right to be forgotten." Council Regulation 2016/679, art. 17, 2016 O.J. (L 119) 43, 44.

98. The power of the "mosaic theory" is not generally appreciated, including by the U.S. Supreme Court. This theory posits that seemingly unrelated pieces of personal information can readily be combined (for instance via data mining software) to create a whole new picture, a picture that reveals private information that the data subject never intended to reveal. This notion is an important part of the discussion about the duration of monitoring a car's movements via a GPS system and what constitutes a Fourth Amendment search and seizure through information collection, as discussed in United States v. Jones, 132 S. Ct. 945, 949 (2012); Matthew B. Kugler, *Surveillance Duration Doesn't Affect Privacy Expectations: An Empirical Test of the Mosaic Theory* (Coase-Sandor Inst. for Law and Econ., U. Chi. L. Sch., Working Paper No. 727, 2015), *available at* http://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=2419&context=law_and_economics.

99. Clicking on a button that says "I agree," as is often done with software "clickwrap" agreements, hardly amounts to bargaining. Nonetheless, cases decided to date generally uphold such agreements as enforceable. *See* ProCD, Inc. v. Zeidenberg, 86 F.3d 1447 (7th Cir. 1996).

100. For example, the Gramm-Leach-Bliley Act of 1999 created some much needed limitations on the transfer of bank customer information to third parties. Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999).

101. For example, the HIPAA of 1996 restricts the types of parties who can receive personal health care

for the most part, information disclosed by third parties to American organizations (for profit, non-profit, and government) becomes the property of the organization to which the information was disclosed. Unless third parties can make a legal claim to some property rights in information about them, it will remain quite difficult for these third parties to legally compel top management to do anything of significance in the information security and privacy area.

There can be no level field bargaining unless consumers have some direct leverage with which to bargain with management. At this time, American consumers have no direct bargaining chips with which force management to adequately protect information and information systems. All consumers have is indirect leverage through exposure in the media and the threat of actions taken by federal or state regulatory authorities.[102] Thus, unless the current legal regime regarding property rights in personal information is going to be dramatically changed (and this does not appear to be happening at any time in the near future), top management must be held personally liable for damage done to third parties because top management has failed to meet the duty of care to these same third parties.[103] The proposed law at the end of this article attempts to achieve this objective: establishing a balanced power between top management and affected third parties by introducing the least possible number of changes in the current legal system.

VII. HOW THE LAW OF AGENCY ACTS AS A COUNTERPRODUCTIVE SHIELD FOR THE BENEFIT OF TOP MANAGEMENT

A. Liability Imposed on the Principal for Torts of the Agent Provides Insufficient Motivation

The outdated understanding of the agency relationship is that top management was the servant (agent) of the board of directors (master).[104] As such, top management should be protected from personal liability by agency law because it

information. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996).

102. One example is provided by state breach notification laws, which due to their inconsistencies and variations point strongly to the need for federal consolidation of legislation in this area. *See*, *e.g.,* Michael Greenberger & Matthew Swinburne, *The Maryland Personal Information Protection Act: Strengthening Maryland's Security Breach Notification Law*, 42 U. BALT. L. F. 129 (2012).

103. Identity theft provides a good example of how consumers have little say over how information about them is controlled or handled; mishandling of this information by a business, and the resulting identity theft, may unjustly cause a consumer to suffer denial of a loan, denial of a job, and additional costs although they were in no way at fault. *See* J. Howard Beales III, *Remarks of J.Howard Beales, III, Director, Bureau of Consumer Protection, Federal Trade Commission, Before the 2003 Symposium on the Patriot Act, Consumer Privacy, and Cybercrime*, 5 N.C. J. L. & TECH 1, 9 (2003).

104. Some definitions are in order per the Restatement (Second) of Agency. A "master" is a principal who employs an agent to perform service in his affairs and who controls, or has the right to control, the physical conduct of the other in the performance of the service. A "servant" is an agent employed by a master to perform services in his affairs whose physical conduct in the performance of the service is controlled or subject to the right to control by the master (note the personal relationship and intimate communication implied by these definitions). RESTATEMENT (SECOND) OF AGENCY § 2 (AM. LAW INST. 1958).

was by implication serving the will of its principal (the board of directors acting for the investors), so long as top management was acting within the scope of its employment.[105] Vicarious liability doctrine imposes liability on the principal (here, the corporation or organizational unit) for the torts of its agents (here, top management). Perversely, this can render the principal in an employment relationship responsible for the self-serving independently chosen acts of an agent. For example, in the context of employment discrimination, employers are legally responsible for the discriminatory acts of supervisory employees, even when the discrimination was the result of a specific supervisor's discriminatory animus which occurred contrary to company policy and without the knowledge of corporate management.[106]

Under common law, an agent-employee (such as a top manager) can be held liable for his own acts, even when an employer (such as the corporation) is also held vicariously liable,[107] but the business judgment rule, which is discussed at length in the next major section of this article, prevents that personal liability for top management from being used in practice. While there is disagreement among the courts[108] about holding agents personally liable for their actions, the prevailing theory, at least in the employment discrimination field, is that the existence of vicarious liability (respondeat superior) creates an incentive for employer principals to manage their agents. This author disagrees, claiming that such a theory creates a significant disincentive for agents to exercise due diligence. Instead, this author proposes a liability scheme that allows joint and several liability, an approach under which both the employer and its agent could be held liable. He suggests such joint and several liability would provide the most influential set of incentives to achieve the desired levels of information security and privacy.

B. Supervision by the Board of Directors Inadequately Controls Activities of Top Management

The shield that the law of agency now provides to top management is predicated on an assumption that the board of directors (representing the shareholders) would actively manage the organization's top managers.[109] While that assumption may have been true in centuries gone past, today it is certainly no

---

105. Scope of employment is addressed in Restatement (Second) of Agency § 2, comment D. As is taken up in greater detail in the following section of this article, the master's liability for acts of its servants is restricted to acts within the scope of employment. RESTATEMENT (SECOND) OF AGENCY § 2 cmt. d (AM. LAW INST. 1958).

106. Meritor Sav. Bank v. Vinson, 477 U.S. 57, 75 (1986); Miller v. Bank of Am., 600 F.2d 211, 213 (9th Cir. 1979).

107. RESTATEMENT (SECOND) OF AGENCY § 343, (AM. LAW INST. 1958).

108. *See* Rebecca Hanner White, *Vicarious and Personal Liability for Employment Discrimination*, 30 GA. L. REV. 509, 549 (1996).

109. Some may wonder why this article does not expressly address the personal liability of members of the board of directors. The short answer is that board members are only tangentially involved in important decisions about information security and privacy. A more lengthy answer is that a substantially different set of laws applies to directors. Consider the "oversight doctrine" which has been manifest in Delaware law. It imposes liability on directors (but not top management) under certain circumstances only if there is a breach of the duty of loyalty. *See* Lisa M. Fairfax, Managing Expectations: *Does the Director's Duty to Monitor Promise More Than It Can Deliver?*, 10 U. ST. THOMAS L.J. 416 (2012).

longer true.[110] The active management influence of boards has dwindled, and top management now largely runs major corporations and government agencies.[111] Operational management and governance, including the ability to make critical trade-off decisions in the domain of information security and privacy, is now attended to by top management, while the board handles only game-changing decisions (such as mergers and acquisitions), strategic direction, and overall policy matters. Thus, boards do not actively manage top management when it comes to information security and privacy.[112] The shots in the area of concern addressed in this article are thus called solely by top management,[113] and it is therefore fitting to hold top management personally liable for markedly deficient information security and privacy that leads to a serious loss. A legislative policy decision to hold top management personally liable is consistent with recent research that shows that corporate wrongdoing, rather than organizational culture, more often results from actions, deliberate or inadvertent, by the top management of the perpetrator organization.[114]

If top management is no longer simply following the orders of the board, then it should no longer be insulated from liability as though it was acting as a "servant," as the law of agency would dictate.[115] Top management instead now acts as though they are operating their own business, much like a sole proprietorship. If a sole proprietorship involves exposure of the owner to liability for the decisions that his or her workers make, why is it that top management in major corporations should be legally insulated from liability[116] for effectively the same actions (especially when the influence of those actions is magnified by scale, as is the case with multinational corporations)? It is the contention of this author that top management should not be so shielded against the effects of their decisions and that to hold them

---

110. Lucian Arye Bebchuk, *The Case for Increasing Shareholder Power*, 118 HARV. L. REV. 833 (2005).

111. This observation is by no stretch of the imagination new and has been discussed for decades, along with conversation about the need for more formal legal acknowledgement of a corporation's duty to parties besides shareholders and creditors. *See*, *e.g.,* E. Merrick Dodd, Jr., *For Whom Are Corporate Managers Trustees?*, 45 HARV. L. REV. 1145 (1932).

112. If one closely examines the current institutional arrangements applicable to large corporations, which have a large number of geographically diverse, often anonymous investors, it becomes quite clear that it is a logistical impossibility for the shareholders (or their representatives on the board) to closely manage top management in most situations, save those where ownership is highly concentrated in a few individuals; the addition of limited liability for investors to induce them to invest discourages shareholders from exercising direct operational control over top management; board consent for top management to serve in a certain capacity should not be equivalent to indemnification of top management for all acts; *see* David A. Westbrook, *A Shallow Harbor and a Cold Horizon: The Deceptive Promise of Modern Agency Law for the Theory of the Firm*, 35 SEATTLE U. L. REV. 1369 (2012).

113. Nicole Beebe et al., *Framing Information Security Budget Requests to Influence Budget Decisions*, 35 COMM. OF THE ASS'N FOR INFO. SYS., 133, 134 (2014).

114. William S. Laufer, *Corporate Liability, Risk Shifting, and the Paradox of Compliance*, 52 VAND. L. REV. 1343, 1411 (1999).

115. *See* Watteau v. Fenwick (1893), 1 Q. B. 346 (finding, under English law, a third party could hold the principal liable for the acts of the agent, even though the agent knowingly disobeyed the principal's instructions, so long as the agent's acts appeared to be within the normal scope of the agent's duties).

116. This author has no problem with the possibility that a principal may be held liable for the acts of its agent under various doctrines such as implied agency, inherent agency, and actual authority. On the other hand, it is a problem when top management acts largely unilaterally but is not held personally liable that an incentive for abuse and/or socially undesirable results is created. For discussions of these three agency doctrines. *See* RESTATEMENT (SECOND) OF AGENCY (AM. LAW INST. 1958).

personally liable encourages appropriate attention to the important tasks of information security and privacy—tasks that are demonstrably not being adequately addressed at the present time.

C. Management Supervision Structures of Early Industrial Age Do Not Scale-Up and Are Still Not Relevant

Another assumption of the current agency law is that the supervision structure, and the inherent legal obligations that were applicable to a sole proprietor and his handful of workers in the 1890s, in the early days of the Industrial Revolution, is still applicable to modern organizations that involve hundreds and even thousands of employees. Here reference is explicitly being made to the shielding the agent has against liability for his acts, because he is, after all, simply operating on behalf of his principal. Such an extreme shield of agents can only work where very close contact between principal and agent is the normal interaction, and great control over the agent can be thereby exercised. This principal-agent supervision and legal obligation model cannot be workable with the scale of modern enterprises such as multinational corporations or industrialized nation centralized government agencies. It is practically impossible to closely manage top management in such a situation where so many parties are involved. This workability problem is exponentially made worse when one considers that the Internet now incorporates a large number of new constituencies, again making the exclusive focus on the intimate old-fashioned principal-agent relationship antiquated, quaint, and totally inapplicable. The only reasonable way forward is to hold top management personally responsible for their personally chosen actions by the law related to negligence and recklessness. That is what the proposed law in the appendix attempts to achieve.

D. "Invisible Hand" of the Marketplace Does Not Cause Imbalances to Be Adjusted Automatically

Still another assumption inherent in the established agency law is that the capitalistic market will automatically adjust with an "invisible hand" to accommodate new conditions.[117] In the information security and privacy field, current events are moving far too fast for us to wait for the market to gradually accommodate and adapt to new conditions. The risks are far too great, and the assets at risk are far too valuable,[118] for this old-fashioned approach to be used alone. Furthermore, the market often relies upon a profound crisis[119] in order to bring about structural change, but this country cannot afford to suffer a still more

---

117. For a critical discussion, *see* E. K. HUNT & MARK LAUTZENHEISER, HISTORY OF ECONOMIC THOUGHT: A CRITICAL PERSPECTIVE 424 (3d. ed. 2011).

118. At this point in time, 88% of the S&P 500's market value is goodwill and intangible assets, such as reputation, brand, and customer experience—all of which are extremely vulnerable to information security and privacy problems. Go back to 1975, and these same assets were only 17% of the market value of these companies. See NYSE & VERACODE, *supra* note 4, at 2.

119. In keeping with this point, many experts in the information security and privacy field believe that significant change in the legal structure surrounding information security and privacy will only come about through a so-called "digital Pearl Harbor" event. *See* SEYMOUR E. GOODMAN & HERBERT S. LIN, TOWARD A SAFER AND MORE SECURE CYBERSPACE 223 (2007), *available at* http://www.nap.edu/read/11925/chapter/15.

severe crisis in the information security and privacy area. This "faith in the market" type of market adjustment is also not happening because there is an insufficient number of readily available market participants to make the theory a reality. For instance, if there is only one cell phone company that offers acceptable service at a customer's house in a remote rural area, then that customer cannot realistically switch service providers in protest about his phone company's negligent handling of his personal data.

Similarly, parties that might create competing business arrangements with preferable allocations of liability are not realistically able to establish their own country where a different set of laws would prevail. The inability of the capitalistic marketplace to deal with situations where no responsibility has been allocated can be found in the "tragedy of the commons" situation mentioned above, where a shared resource is accordingly degraded or even destroyed, because responsibility for the management of that resource is not explicitly assigned to certain parties. Indeed, as discussed above in the sections about incentive systems, even though the efforts of top managers are urgently needed to solve this problem, top managers personally benefit under the current legal system if they continue to follow a process characterized by inaction in the information security and privacy area.

Even if the reader were a firm believer in the efficiency of the marketplace and its adaptability, there is still a place for the integration of moral codes into the law. Doing what is right for society as a whole, in this context ensuring that the information systems on which we all depend include adequate security and privacy, that objective seems to be a relatively easy moral code behind which most people could align.[120] Thus, the law now needs to be adjusted to accommodate the new conditions, and lawmakers and policymakers should not assume that the marketplace is infinitely self-adaptive.[121] In some areas, intervention is necessary, and based on the emergency conditions that now prevail, information security and privacy is one of those areas in which legal intervention with the mechanisms of the market is required.

E. Important Management Tasks Cannot Remain Unassigned Without Causing Significant Adverse Repercussions

Rather than being an explicit assumption, perhaps it would be better to call this next topic an area of unconsciousness in need of more explicit attention. There appears to be an all-too-common default belief in the legal and business communities that it is acceptable, indeed even workable, for important tasks to remain unassigned to specific individuals. This practice is contrary to generally

120. For a discussion about the morality associated with leaving such decisions to the market, *see* BERNARD HODGSON, THE INVISIBLE HAND AND THE COMMON GOOD (2004).

121. The need for major changes in the law to deal with the new information security and privacy risks is recognized by other English common law countries, such as Australia (which is considering the introduction of a new tort, but this article takes a more conservative approach, opting instead to adjust the existing negligence and recklessness laws so as to accommodate new conditions); *see* AUSTL. L. REFORM COMMISSION, SERIOUS INVASIONS OF PRIVACY IN THE DIGITAL ERA (2014), *available at* https://www.alrc.gov.au/publications/1-executive-summary/should-new-tort-be-enacted.

accepted accounting principles,[122] just as it is contrary to generally accepted information systems security and privacy practices.[123] Consistent with that assumption, or perhaps "consistent with that unconsciousness," assignment of liability-related responsibility for information security and privacy is still nebulous and ill-defined.[124] While it is acknowledged that this is a new field and both the legal and business communities are understandably still adapting to information security and privacy, explicit assignment of legal responsibility is now urgently needed.[125] The draft law proposed in this article is an attempt to obtain explicit assignment of responsibility of liability to top management because it is clearly the single group in a position to most effectively improve the current state of affairs. Management studies have clearly shown that by assigning responsibility and accountability, desired behavior is encouraged and motivated.[126]

VIII. HOW THE BUSINESS JUDGMENT RULE ACTS AS A COUNTERPRODUCTIVE SHIELD FOR THE BENEFIT OF TOP MANAGEMENT

A. We Must Admit the Total Insufficiency of Top Management Knowledge in This Area

The business judgment rule is defined in many different ways,[127] but in general terms, it holds that top managers will not be held personally liable for the results of a business decision if the defendant top managers: (1) were not personally interested in the subject matter and made the decision in good faith, (2) were reasonably informed about the subject matter to the extent that they deemed necessary under the circumstances, and (3) rationally believed that the choice made was in the best interests of the organization.[128]

One the most serious problems with the business judgment rule is found in the second element, which involves management's thought and belief about the extent to which the state of being informed has been achieved, or the state which is required in order to make this particular decision. To use top management's thought and belief as a reference point is not only arbitrary and difficult to ascertain

---

122. COMMITTEE ON GOV'T AFFAIRS, 95TH CONGRESS, IMPROVING THE ACCOUNTABILITY OF PUBLIC OWNED CORPORATIONS AND THEIR AUDITORS 6, (Comm. Print 1977).

123. NAT'L BUREAU OF STANDARDS, AUDIT AND EVALUATION OF COMPUTER SECURITY II: SYSTEM VULNERABILITIES AND CONTROLS §4.1.5 (1980).

124. Christopher McClean, *The Hacking Economy: Five Things the Sony Hack Exposed*, CNBC (Dec. 30, 2014, 2:49 PM), http://www.cnbc.com/2014/12/30/5-things-the-sony-hack-exposed-commentary.html.

125. This claim is consistent with the very important work being done by the Information Systems Audit & Control Association (ISACA), as exemplified in their report, INFORMATION SECURITY GOVERNANCE: GUIDANCE FOR BOARDS OF DIRECTORS AND EXECUTIVE MANAGEMENT (2d ed. 2006); *see also* David Orozco, *Amending the Economic Espionage Act to Require the Disclosure of National-Security Related Technology Thefts*, 62 CATH. U. L. REV. 877, 900 (2013) (discussing the nebulous nature of this area of the law).

126. *See*, *e.g.*, Jesse W. Brogan, *Improving Lean Six Sigma Process with Lean Six Sigma*, iSIX SIGMA, http://www.isixsigma.com/implementation/deployment-structure/improving-lean-six-sigma-process-lean-six-sigma (discussing industrial engineering and quality control, and the importance of assigning responsibility and accountability).

127. *See*, *e.g.,* MODEL BUS. CORP. ACT § 8.30(a) (1994).

128. PRINCIPLES OF CORPORATE GOVERNANCE: ANALYSIS & RECOMMENDATIONS § 4.01(c), (1994).

empirically in a trial, but it is also going to inevitably dangerously expose not just the organization itself, but also third parties to unnecessary vulnerabilities. This undue exposure results from the fact that top management is not aware of the latest threats, problems, management techniques, and issues in the information security and privacy fields.

It is not top management's job to stay on top of such matters, and it would be unrealistic to expect that they would devote the time necessary to stay on top of the latest in the information security and privacy areas, given the highly demanding nature of their actual jobs. At the same time, to provide an adequate level of information security and privacy, the organization that top management oversees, must employ an "on top of the latest" approach to information security or privacy, or the organization will soon be victimized by hackers, industrial spies, disgruntled ex-employees, organized criminals, hostile nation state actors, and other adversaries.

So the reference point for determining whether information security is adequate must be built upon a demonstrably verifiable external standard, that reflects the latest developments, and that can be attested to by independent third party experts. Such an approach has been shown to be useful in the publicly released financial statements area,[129] via the use of Certified Public Accountants providing a professional opinion based on an independent audit. That same third party expert opinion approach can and should be applied to the information security and privacy field as well. The law in the appendix to this article takes that same approach, and the business judgment rule must be restricted so as to limit management's thoughts and beliefs to those matters that are demonstrably consistent with independent third party expert opinion. One example of such a restriction of the business judgment rule is found in the draft law found in the appendix to this article.

B. We Must Also Admit the Courts Cannot Reasonably Assess Conflicts in this Area

Another serious problem associated with the business judgment rule, as evidenced by the first element in the definition of that rule provided above, is that the rule assumes that the courts can reasonably assess[130] whether top management is interested, i.e., whether they have a conflict related to the decision to be made.[131] Not only is this unduly consuming of limited court resources, in opposition to the much bandied-about legal objective of judicial economy, but to suppose that management could be unconflicted and uninterested is contrary to the evidence discussed earlier in this article which delves extensively into the dysfunctional

129. For a demonstrably useful example of the type of third party reviews that could be applied to the information security and privacy area, *see* AMERICAN INSTITUTE OF CERTIFIED PUBLIC ACCOUNTANTS, CLARIFIED STATEMENTS ON AUDITING STANDARDS (2015), http://www.aicpa.org/Research/Standards/AuditAttest/Pages/clarifiedSAS.aspx.

130. Of course, the court does not want to make this assessment either for reasons of judicial economy, if for no other reason. Courts are also generally run by lawyers (acting as judges), and those people in general have no special expertise in either modern management nor in technology.

131. One of the leading decisions in this area is Weinberger v. UOP, Inc., 457 A.2d 701 (Del. 1983), in which the court emphasized that it is critical that directors operate with the "utmost good faith and the most scrupulous inherent fairness." *Id*. at 710.

incentive systems now in place.

Top management is clearly now incentivized to focus on the short-term, high-bonus-producing, quick results solution, and not the long-term investment that is needed, or the difficult and time-consuming area now urgently in need of much more of their attention. The fact that many buy-out deals and other major corporate merger and acquisitions transactions now involve review by separate committees is evidence that a third party independent viewpoint is needed.[132] The need to appear to have integrity and independence is evidence with these special committees, and they would not be used as a standard practice unless management conflicts and personal interests were not serious issues.[133]

C. We Must Admit that the Line Was Improperly Drawn at Lack of Fraud, Bad Faith, or Other Nefarious Intentionality

Still another problem with the business judgment rule is that it allows top management to evade liability, so long as their unwise decisions or other wrongdoings are not intentional.[134] These days, it is not enough to simply require that there be no intentional misconduct.[135] Today, with the incredible powers and responsibilities that go along with being a top manager at a major corporation, a large government agency, or a well-known major non-profit, there must be liability exposure for not adequately attending to the important needs of third parties, such as properly protecting the information security and privacy of these third parties.

For example, should the top management decisions that allowed the Sony Pictures hack to take place, a hack which cost the studio at least $15 million,[136] simply be passed along to the shareholders without any contributory payments from top management? The total loss amount sustained by Sony as a result of the hack is peanuts compared to the massive losses that we, as a society, now potentially face because top management made unintentional and unwise short-term decisions related to information security and privacy. Clearly, "it wasn't intentional" should not be a permissible excuse with which to dismiss management personal liability.

---

132. *See* Scott V. Simpson, *The Emerging Role of the Special Committee – Ensuring Business Judgment Rule Protection in the Context of Management Leveraged Buyouts and Other Corporate Transactions Involving Conflicts of Interest*, 43 BUS. LAW. 665 (1988).

133. In certain circumstances, courts have found that the business judgment rule does not protect the directors or top managers, and that there has been a breach of the duty of due care, and that directors or top management should thus be held personally liable for damages. *See* Smith v. Van Gorkom, 488 A.2d 858 (Del. 1985). Likewise, the draft law in this article seeks to hold top management personally liable.

134. *See* Kamin v. American Express Co., 383 N.Y.S. 2d 807 (App. Div. 1976). This case involved the directors making a decision which cost the shareholders a great deal of money, but since there was no fraud or self-dealing shown by the plaintiff shareholders, no award to the plaintiffs was provided. In the words of the court, "more than imprudence and mistaken judgment must be shown" thanks to the business judgment rule. *Id*. at 813.

135. *See* Otis & Co. v. Pennsylvania R. Co., 61 F.Supp. 905 (E.D. Pa. 1945). The old fashioned view was evident in this case, where the court reasoned that "mistakes or errors in the exercise of honest business judgment do not subject the officers and directors to liability for negligence in the discharge of their duties." *Id*. at 911.

136. Cecilia Kang, *Sony Pictures Hack Cost the Movie Studio at Least $15 Million*, WASH. POST (Feb. 4, 2015), www.washingtonpost.com/news/business/wp/2015/02/04/sony-pictures-hack-cost-the-movie-studio-at-least-15-million.

Top management discretion needs to be narrowed, and making serious errors or omissions in the information security and/or privacy area should no longer be excused because negative intentionality is missing.[137]

D. We Must Acknowledge that the Message Sent to the Public Is Inadequate & Itself Doing Harm to the Public Trust in Modern Institutions

When so few American top managers are held personally responsible[138] for the wrongdoing of their corporations, what kind of a message does that send to the public?[139] Rather than indirectly sending the message that those at the top can now get away with such crimes and torts,[140] a good argument can be made for increasing the severity of penalties resulting from the number of people affected, the amount of money involved, the abuse of power by top managers, and the reputational damage to the organization in question.[141] Socially, it is considered worse when a leader establishes a low standard for the organization's norm because others follow that leader. Therefore, if a top manager has been involved in criminal or abusive conduct, that conduct should be severely penalized.

A good argument can also be made for severe penalties because top management is, due to their great wealth relative to the rest of the population, not incentivized unless they suffer a very significant personal loss of wealth. Making the personal liability risk that top management potentially faces very severe can counter the fact that third parties have no legal basis for negotiation in the decisions that top management is making about information handling and information systems—decisions that affect those same third parties profoundly.

There is a counterargument against increasing liability exposure for top management that claims that corporations are better able to handle the greater liability exposure that goes along with today's multinational corporations and other large organizations. While it is true that the corporation, government agency, or non-profit organization involved may have deeper pockets than top managers, the

---

137. *See* Leslie v. Lorillard, 110 N.Y. 519, 532 (1888). The old-fashioned view embodied in that case now must be changed. That court wrote "mere errors of judgment are not sufficient as grounds for equity interference [establishing a violation of a duty of care]; for the powers of those entrusted with corporate management are largely discretionary." *Id*. at 532. We must now move beyond discretionary powers granted to top management, and hold top management to a standard of due care that can be established via external sources such as expert testimony.

138. *E.g.,* FDIC v. Castetter, 184 F.3d 1040 (9th Cir. 1999). In that case, bank directors were not held personally liable for acting negligently and causing their bank to fail because the business judgment rule set the negligence standard high (effectively gross negligence), and the directors therefore were deemed to be not guilty.

139. In 2014, some 75% of the general public surveyed in a poll said they see widespread government corruption, so it would be naïve to believe that there is not a serious perception issue in this area (this is markedly up from 2009 when 66% felt the same). 75% in U.S. *See Widespread Government Corruption*, GALLUP.COM (Sept. 19, 2015), http://www.gallup.com/poll/185759/widespread-government-corruption.aspx.

140. Even those living in foreign countries comment on how American executives seem to "get away with it" these days. *See* Joris Luyendijk, *Now the Bankers' Triumph is Complete*, GUARDIAN (Jan. 22, 2016), http://www.theguardian.com/commentisfree/2016/jan/22/bankers-triumph-complete-the-big-short.

141. *See generally* Harold G. Grasmick & Donad E. Green, *Legal Punishment, Social Disapproval and Internalization as Inhibitors of Illegal Behavior*, 71 J. CRIM. L. & CRIMINOLOGY 325 (1980) (finding that internalization, social opprobrium, and official penalties all had a significant impact when it comes to influencing criminal behavior).

corporation is not making the decisions and it is not incentivized to act one way or another, unlike top managers. Furthermore, nothing in the proposed law found in this article eliminates or changes the doctrine of respondeat superior,[142] so the corporation (or other organizational entity) can still, at least in theory, provide additional assets to help settle the claims of third parties were they to be damaged by the information security and privacy related crimes or torts of top management.

E. An Adjustment for the Lack of a Third Party Voice is Now Required

Furthermore, to hold the shareholders solely liable for disastrous decisions involving information security and privacy, decisions over which the shareholders had little or no influence, is not just ineffective, but inequitable. While shareholders may diversify away some of this risk by making multiple investments in different organizations in an effort to reduce their potential adverse personal consequences, top management by design cannot diversify away the personal liability exposure that they face through a law such as the one provided in the appendix to this article. That is desirable because top management must be constantly facing the prospect of losing everything they own because they were negligent or reckless when it comes to information security and privacy. The safe harbor rules described in this draft law are relatively clear and straightforward, and top management can, in fact, readily make sure that they will not be hit with a successful negligence or recklessness civil lawsuit or criminal prosecution under this draft law. Therefore, compliance with such a law would actually not be an onerous proposition, while non-compliance would, in contrast, bring extreme and unnecessary risk, a risk that every rational top manager would refuse to accept. The relative risk exposure associated with compliance and non-compliance, in turn, should motivate top management behavior to properly look after the needs of third parties in the area of information security and privacy.

Thus, we come back to the critical distinction between bearing risk for unintentional acts and bearing risk for intentional acts. The corporation is the better entity to bear risk for unintentional acts, while top management is the better entity to bear the risk for knowing and intentional acts.[143] On balance, greater harm would result, and top management would be less motivated to act in a socially-minded manner if the risk was to be borne solely by the organization rather than by both the organization and top management personally.[144] Accordingly, the draft law in this article was written with the intention of deterring bad behavior on the part of top

---

142. RESTATEMENT (THIRD) OF AGENCY § 2.04 (AM. LAW INST. 2006) (translating respondeat superior into English, specifying it means, "let the master answer;" in the employment context, an employer is subject to liability for torts committed by employees while those employees are acting within the scope of their employment).

143. Vikramaditya, *supra* note 30, at 1254-55.

144. *See* V.S. Khanna, *Corporate Criminal Liability: What Purpose Does It Serve?,* 109 HARV. L. REV. 1477, 1496-97 (1966). Shareholders have not historically been able to manifest sufficient visibility and monitoring of top management activities so as to be able to control top management activity in this area, specifically so as to motivate top management not to take undue risks with the corporation's assets. While shareholders could theoretically modify top management employment contracts to include such incentives, to date, there has been scant real world action this area, and the possibility remains but a theory.

management,[145] setting an example of those top managers who abuse their position, and forcing top management to take right actions.

F. An Externally Defined Standard of Due Care Is Now Essential

While the notion of a fiduciary duty to shareholders and the doctrine of respondeat superior, both discussed above, imply a duty of care to which top management must subscribe, it should be noted that that duty is to the shareholders, donors, taxpayers, or other primary constituency that the organization serves. The duty of care for top managers, however, is not currently owed to third parties, but as discussed at length at the beginning of this article, it must now – given our new inter-connected industrial society information systems infrastructure (such as the Internet) – also be owed to third parties who have a relationship with the organization, third parties who could be adversely impacted by decisions that top management makes in the information security and privacy field. Having a legally-defined, expert-vouched duty of care to the constituencies served is common to many professionals, such as accountants, lawyers, architects, engineers, and medical doctors.[146] Why then are top managers in corporations not also subject to having their duty of care defined by the externally-referenced standard of due care? Tradition and history could be offered up as explanations, but top managers having only a legally recognized loyalty to their employer (the organization and its owners) must now change.

Continuing with the need for an externally-referenced and expert-vouched standard of due care for top management, one should note that two of the three elements in the business judgment rule are determined by the defendant top manager. Notably, the top manager must (1) have made a reasonably informed decision[147] – as he or she would believe that level of being informed to be – as established by a very low gross negligence standard, and (2) the top manager must have some rational belief that the decision was in the organization's best interest – established by a very low threshold, essentially not totally beyond the bounds of reason.[148] That two of the essential three elements in the business judgment rule allow the defendant to make up their own story about how he or she has met the standard of proper conduct is totally unacceptable in this day and age when so much is riding on top managers making the right decisions. This type of self-evaluation invites not just unwarranted excuse, but also abuse, and provides scant protection of third parties who must be protected. Top management must now be subject to an externally defined standard of due care, as is suggested in the draft law at the end of this article.

---

145. The single most important factor associated with allocating liability between the corporation, top management, and injured third parties is the degree of care exercised by the enterprise and by the agent. *See* Lewis A. Kornhauser, *An Economic Analysis of the Choice Between Enterprise and Personal Liability for Accidents*, 70 CALIF. L. REV. 1345 (1982). Note that this article advocates neither agent liability alone, nor enterprise liability alone, instead suggesting that liability of both brings about superior long-run socially-desirable results.

146. *See* H. H. Henry, *Annotation, Necessity of Expert Evidence to Support an Action for Malpractice Against a Physician or Surgeon*, 81 A.L.R.2d 597 (1962).

147. Aronson v. Lewis, 473 A.2d 805, 812 (Del. 1984).

148. Cuker v. Mikalauskas, 692 A.2d 1042, 1045 (Pa. 1997).

G. Existing Moral Hazard Must Be Removed

Before leaving the topic of the problems associated with the business judgment rule, the moral hazard[149] associated with holding only an entity liable for the acts of its top management that damage third parties should also be mentioned. Vicarious liability alone, where the organization is held liable for the criminal or abusive acts of top management, will incentivize top management to engage in more acts of that nature.[150] This is because top management does not personally pay the price, and if they can personally reap the benefits (for example through higher quarterly bonuses, as discussed earlier in this article), then they will seek out arrangements that will allow them to strike such deals and engage in such arrangements.

Shifting of the responsibility to the organization encourages the view that this area should be handled with risk management, for example with insurance,[151] rather than by designing incentive systems that motivate top management to act in a manner that helps to assure that adequate information security and privacy are provided. After the risk is transferred, for example to an insurance company, the incentive to maintain high levels of care is likely to markedly decrease.[152] The draft law found in this article is designed to keep top management incentivized to provide funds and attention to achieve adequate levels of information security and privacy. Insurance, use of outsourcing firms, and other methods for information security and privacy related risk transfer can still be employed, if such a law were to be enacted, but these risk transfers would not then be serving to disincentivize top management because the accountability would still rest with the decision makers, the top managers.

IX. WHY THE ASSUMPTION OF RISK DEFENSE SHOULD BE SEVERELY LIMITED IN THIS AREA

The assumption of risk defense to negligence and recklessness is predicated on having a level playing field, where both parties have information about the other, so as to be able to make a reasonably educated decision.[153] This type of disclosure

149. William S. Laufer, Corporiate *Liability, Risk Shifting, and the Paradox of Compliance*, 52 VAND. L. REV. 1343 (1999).

150. *See* Unocal Corp. v. Mesa Petroleum Co., 493 A.2d 946 (Del. 1985). This case is particularly noteworthy because the court said that the duty of care in takeover situations is higher ("enhanced") than it usually is because there are moral hazards in those situations, and additional requirements will thus be required in order to ensure that top management acts in a manner that maintains the best interests of the shareholders. As discussed in this article, a heightened duty of care is now needed in information security and privacy matters, and the proposed law in the appendix to this article suggests one way to go about establishing that heightened duty of care.

151. Empirical research shows that even though insurance companies ultimately pay the costs caused by negligent top management, when directors' and officers' insurance is in force, they do not effectively monitor top management corporate governance. *See* Tom Baker & Sean J. Griffith, *The Missing Monitor in Corporate Governance: The Directors' & Officers' Liability Insurer*, 95 GEO. L.J. 1795 (2007). Additionally, once litigation has begun, insurance companies do not manage litigation defense costs either. *Id*. These findings mean that insurance companies are not in a position to motivate top management to perform the necessary tasks to prevent harm to third parties. The findings also imply that the deterrent effects of shareholder derivative suits and regulatory actions are less than what is generally believed.

152. *See* Steven Shavell, *On Moral Hazard and Insurance*, 93 Q. J. ECON. 541 (1979).

153. *See* RESTATEMENT (SECOND) OF TORTS § 523(c) (AM. LAW INST., 1977) (stating that a plaintiff does

might prevail when two firms are going through a merger or acquisition, or some other very close type of engagement, perhaps a joint venture. But for the most part, even business partners are unaware of the information security and privacy at other firms with whom they do business. This is because maintaining confidentiality of the actual information security and privacy activities provides another level of security. Maintaining this level of confidentiality,[154] even doling out information on a "need to know basis," is considered standard business practice, even with business partners.

Such information about information security and privacy at the organization in question is even less likely to be disclosed to a customer, taxpayer, donor, shareholder, or another person in a similar position, even if these parties have a demonstrable business relationship with the organization in question. Arguably, these third parties have a right to know how their personal information is being protected. A prospective customer who is interacting with a business and is about to subscribe to or purchase a product or service will have even less information about the state of information security and privacy at the business. Accordingly, such a person cannot reasonably assume the risk, because he does not know what the risk entails. Therefore, the use of the acceptance of the risk defense in negligence and recklessness cases should be limited to those circumstances in which the plaintiff knew about the nature of the risks and voluntarily chose to accept those risks.[155] The draft law in this article attempts to embody wording to that same effect.

X. WHY CONTRIBUTORY NEGLIGENCE SHOULD SIMILARLY BE SEVERELY RESTRICTED IN THIS AREA

The distinction between assumption of the risk and contributory negligence is vague, but operationally a distinction can be drawn in that assumption of the risk is a voluntary choice made by the plaintiff and that choice is later used as an affirmative defense that would deny or restrict the liability of the defendant. On the other hand, contributory negligence involves some negligence or conduct, that an "ordinary man" would reasonably avoid, conduct committed by the plaintiff, and that negligent conduct is used as a method for reducing damages to be paid by the defendant, based on the observed relative misconduct of the parties to the lawsuit.[156]

The common law defense involving contributory negligence revolves around the rule that there can be no recovery of damages for negligence if the injured person, by his own negligence, or by the negligence of another that is imputable to

not assume the risk unless he knows of its existence).

154. This approach is often called "security by obscurity," and while it should not be the only type of security of information employed, it can be a useful adjunct to other deployed controls, when used in a "defense in depth" (multiple layers of controls) approach. For example, the U.S. military uses this approach by not publicly revealing the encryption algorithms that it employs for its current deployments.

155. *See* Dura Corp. v. Harned, 703 P.2d 396 (Alaska 1985). In this case, the court found for the plaintiff in a product liability matter, and acceptance of the risk was not permitted as a defense because the plaintiff, who was injured due to the lack of a safety device, did not know that the device was missing.

156. Mumma v. Reading Co., 247 F.Supp. 252, 257 (E.D. Pa. 1965).

the injured person, proximately caused the injury. But in the context of an average third party who may be harmed by the information security and privacy choices made by top management, it is hard to understand how the third party could have sufficient information so as to be reasonably informed about the risks and avoid them. Again, for the reasons stated in the prior section's discussion about assumption of the risk, if the organization's information security and privacy activities remain unknown to the third party, and the third party cannot understand the risks, then there can be no rational use of the doctrine of contributory negligence.

Negligence involves the notion that there has been some misconduct, but if a third party is compelled to be involved in a business process, in order to maintain his or her job for example, there can be no contributory negligence.[157] This is because participation in a business process, to which the information security and privacy risks imposed by top management decisions apply, is not a choice made by the involved third party. If participation is forced as a requirement of a job, or in order to obtain a social service, or some business related product or service, the third party cannot be said to have chosen to engage in misconduct, because his or her participation was effectively forced. In the latter circumstances, use of the doctrine of contributory negligence should be denied by the presiding judge. Thus, the only permissible use of contributory negligence should be when the plaintiff voluntarily accepted the danger, and such a danger was clearly out of all proportion to the interest that he or she sought to advance through the choice to accept the danger.[158] Where the situation was not clearly in proportion in the eyes of the plaintiff, then an assumption of the risk defense might still apply, as taken up in the prior section of this article. The draft law found at the end of this article attempts to embody these ideas.

XI. HOW THE AFFIRMATIVE DEFENSE OF LICENSE MUST LIKEWISE BE SEVERELY RESTRICTED IN THESE CIRCUMSTANCES

The affirmative defense of license provides that the defendant had permission from the plaintiff, to engage in the conduct that is set forth in a complaint.[159] The defendant's conduct, which the plaintiff believed to constitute a tort or some other unlawful conduct, is thus alleged to be permissible because it was contractually agreed-upon in advance. This defense is predicated on a pre-existing contractual agreement, and should at least in theory be permissible according to the freedom to contract doctrine,[160] as supported by the Fourteenth Amendment to the United States Constitution. Effectively, such a contractual agreement provides a promise

157. *See* Pritchard v. Liggett & Myers Tobacco Co., 350 F. 2d 479 (3d. Cir. 1965).

158. *See* RESTATEMENT (SECOND) OF TORTS § 496A cmt. c (AM. LAW INST. 1965) (comparing unreasonable assumption of the risk with contributory negligence).

159. Peter J. Shurn III, *Potential Pitfalls of High-Tech Copyright Litigation*, 25 J. MARSHALL J. COMPUTER & INFO. L. 513, 530 (2008).

160. *Compare* Lochner v. New York, 198 U.S. 45 (1905) (holding that freedom to contract was implicit in the Fourteenth Amendment due process clause), with West Coast Hotel Co. v. Parrish, 300 U.S. 379 (1937) (taking a much less activist role and permitting many more regulations). The latter pro-regulatory federal government attitude is assumed to continue and be conducive to passing and upholding the draft statute found in the appendix to this article.

not to sue the defendant.[161] When the defendant's conduct is outside the scope of the license provided,[162] then an infringement of the plaintiff's rights, or an actionable tort of some sort, may have occurred, and this affirmative defense would not apply.

However, the license defense is predicated on an assumption that does not hold up in the real world, namely that a business, non-profit organization, or government agency offering a product or service that has the opportunity to purchase the best legal talent that money can buy is on an equal playing field with a consumer, who in all likelihood has not even read the terms of service (TOS), the legal contract, or the other agreement to which he or she must accede in order to obtain the sought-after goods or services. Further, the average consumer does not have access to the best legal talent available, nor does he or she have any preconceived notion that to engage such sophisticated legal talent– even if he or she was in a position to pay for it– would make a difference. The situation bears much resemblance to an "adhesion contract." Thus, there is no bargaining possible in these situations and therefore there can be no "meeting of the minds." Without a meeting of the minds on all material facts, however, there can be no contract.[163] Therefore, license should not be recognized as an affirmative defense against information security and privacy related negligence or recklessness, unless the parties truly have both a meeting of the minds and a comparable level of power in the negotiations (more colloquially called a "level playing field").

One illustrative case revealing the inequities in this problematic area of the law and the new types of information to which rights and obligations have not yet been legally formalized is found in a case where medical researchers used cells from a patient's body without his permission.[164] The patient sued the researchers claiming conversion, alleging that they used his cells for lucrative research purposes that were not expressly agreed upon. While the court did find insufficient disclosure on the part of the medical researchers, it denied legal recognition of a patient's right to his own cells after they left his body and denied any recovery for conversion.

This case is analogous to what is happening in the information security and privacy field, because in America today, new types of personal information and new uses for such information are being discovered and commercially exploited, largely without the consumer's or data subject's consent. The lack of specific knowledge and ability to effectively negotiate, as manifest in adhesion contracts and other so-called licenses, should not permit commercial, governmental, or non-profit interests to exploit the rights and information of others to the detriment of the individuals involved. In the aforementioned case, it is notable that the court wrote that the plaintiff could not "state a case for conversion under existing law." New laws, such as the draft law found in the appendix to this article, need to be enacted

161. FED. R. CIV. P. 8(c).

162. One case where this affirmative defense was used successfully involved a database and the taxonomy employed in that database. *See* Edgenet, Inc. v. Home Depot, 658 F.3d 662 (7th Cir. 2011). In that case, the database customer's use of the taxonomy was permissible per the contract, even though the taxonomy was protected by copyright and customer no longer subscribed to the database service.

163. Smith v. Neilan, 205 N.W.2d 186, 188 (1973) (denying specific performance under a contract because there was no meeting of the minds in the contract).

164. *See* Moore v. Regents of Univ. of Cal., 793 P.2d 479 (Cal. 1990).

so that plaintiffs are able to state their case under existing laws.

XII. HOW THE COMMON LAWS OF NEGLIGENCE AND RECKLESSNESS SUPPORT A NECESSARY REBALANCING OF LIABILITY RELATED INCENTIVES

A. Compliance-Related Fixed Law & Regulation Alone Cannot Be Effective

The American information security and privacy approach, adopted by both private organizations, such as credit card companies, and government agencies, such as bank regulators, is focused primarily on compliance with laws and regulations. This approach can be mandated by government legislators or regulators, or by private-party contract.[165] Without question, a great deal can be achieved with laws and regulations that specify what needs to be done, but too much faith is being placed in this compliance strategy.[166] What is urgently needed is a shift of the focus to include greater organization-specific risk management. By adopting laws that revitalize negligence and recklessness, as the proposed law in this article does, both the country and the organizations within it can achieve the desired shift to more risk management.

The great emphasis on compliance has failed because it is unduly complex, burdensome, and fixed. For instance, at the time that the Sony Pictures hack took place (the incident mentioned at the beginning of this article), the firm was in compliance with the PCI security standard.[167] That notable achievement did not, however, prevent very serious damage. By shifting the emphasis away from regulation and onto risk management, top management will be forced to take more of a holistic viewpoint that responds to the unique needs of their own organization, instead of the artificially imposed requirements dictated by some legislator or regulator at a considerable time in the past.

The compliance model for dealing with information security and privacy labors under the false assumption that this exceedingly complex field can be properly addressed through a one-size-fits-all solution. That's like trying to get a square peg to fit in a round hole, or actually a hole that is very much more complex than simply round. Only top management knows exactly what an organization's true information security and privacy requirements are from a risk management perspective, and they should thus be held accountable to make sure that the controls that are installed and operated are, in fact, those dictated by the organization's unique needs, not just those imposed by compliance related laws and regulations.[168]

---

165. For example, merchants accepting credit cards must comply with the Payment Card Industry Data Security Standard, also known as being "PCI Compliant." If a firm wishes to accept, process, store or transmit credit card data, it must sign a contract that includes compliance with this standard as well as regular audits.

166. There is evidence of an increasing appreciation inside the information security and privacy community, that compliance alone is not sufficient, and so a second line of defense is needed, which can be provided by risk management. For example, the Office of the Comptroller of the Currency (OCC), a U.S. bank regulator, has issued guidance urging banks to adopt risk management processes. *See Third-Party Relationships: Risk Management Guidance*, OFFICE OF COMPTROLLER OF CURRENCY: OCC BULLETIN 2013-29 (Oct. 30, 2013), http://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html.

167. *See* PCI SECURITY STANDARDS COUNCIL, PCI DSS QUICK REFERENCE GUIDE: UNDERSTANDING THE PAYMENT CARD INDUSTRY DATA SECURITY STANDARD VERSION 2.0 (2010).

168. *See* David Thaw, *The Efficacy of Cybersecurity Regulation*, 30 GA. ST. U. L. REV. 287 (2014).

It is presumptuous for legislators, regulators, or third parties of any type to assume that they know what organizations must have in order to be secure. Thus the compliance-related approach, if relied upon completely, cannot help but be deficient, and the predictable result will be serious compromises of security and privacy.

Unless primary reliance on compliance is significantly changed, as this article suggests, and as long as the information security and privacy problems get worse[169]—which they have progressively done for the last several decades—progressively greater emphasis will be placed on compliance, and the costs and burdens on management's time imposed by compliance requirements will get progressively greater for organizations. Much of this cost and time required for compliance is wasted because the burdens imposed by the laws and regulations are inapplicable to the organizations in question. Still more frustrating is the fact that these wasted resources could have alternatively been devoted to the true information security and privacy needs of the organization. This would have been the case if an emphasis on risk management had been adopted, as in keeping with the proposed law at the end of this article.

The compliance approach should not be entirely abandoned, because significant improvements to information security and privacy has resulted from compliance-related efforts. But the approach to compliance is going to become more granular, for example industry specific, rather than the coarse general approach that has been ill fitting to the needs of many organizations. Rather than dictating specific control measures, technologies, or procedures, more emphasis must be placed on general methodologies, policies, and goals. The work of the Federal Trade Commission is exemplary in this respect because it has, for example, been using the goal of stopping "unfair and deceptive acts and practices" as a way to achieve many positive information security and privacy goals.[170] Its work has helped a great deal to make sure that the public representations of organizations, for example in web-posted privacy policies, are consistent with the ways the involved personal information is being protected by the organization in question.

While some proponents of the compliance-related approach to solving the information security problem are taking a very dictatorial approach[171] to what management must do and how they must do it, such an approach is incompatible with the free market system and the basic economic axiom that the free market should be able to determine how best to meet consumer needs. Accordingly, the law proposed herein specifies only the basic needs, it does not specify how management has to meet those needs. Management in each organization will know

169. Organizations are now seeing a proliferation of compliance-related laws and regulations at both the state and the federal levels. For example, consider the laws regarding reporting security and privacy breaches, which are a mess of confusing requirements coming from many different jurisdictions. *See* NAT'L CONFERENCE OF STATE LEGISLATURES, SECURITY BREACH NOTIFICATION LAWS (2016), *available at* http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx. In the overall information security and privacy area, a unified federally-dictated approach is urgently needed, and it is the law proposed by this article that points in the direction where the nation must go in order to rationalize, clarify, and simplify these laws and regulations.

170. *See* 15 U.S.C. § 45(a)(1) (2006).

171. *See* Cary Coglianese & David Lazer, *Management-Based Regulation: Prescribing Private Management to Achieve Public Goals,* 37 L. & SOC'Y REV. 691 (2003).

best how to meet those needs, rather than government actors taking the role of a parent supervising a child's every move. There are some basic needs which must be met, such as taking care of the security and privacy needs of third parties, which can be handled with a negligence and recklessness-related duty of care, and those basic requirements are set forth in the proposed law found in this article, but legislation and regulation of this nature should not be very detailed lest it become counterproductive. In that respect, this author is advocating for the performance-based approach to compliance so that only the final desired state is mandated by laws and regulations.

Another reason why the emphasis on the compliance approach to information security and privacy is not advisable is that it can encourage a regulatory "race to the bottom" between states.[172] Although it is not yet a notable problem, except perhaps in the breach notification area, this intention by states to attract or retain economic activity by liberalizing laws and regulations is not a good thing for information security and privacy. Such an approach would encourage states to specify only the bare-bones requirements so that they can attract businesses to their state, in effect, placing revenue generation above the public welfare.[173] The problem with state competition based on regulatory or legal minimization is that the Internet has globalized markets, and the balkanization of information security and privacy regulation only results in undue burdens and unnecessary costs for the organizations required to comply with these laws and regulations specified by many different jurisdictions. Ultimately, we will need a worldwide approach to such matters, but a proper step to take at this point in time is to have unifying and consistent federal legislation to standardize the laws and regulations within the United States.[174]

B. Demonstrated Dynamic Adjustment Inherent in Common Law

The common law related to negligence and recklessness does not presuppose that people will always be protected. Likewise, it is realistic to believe that information security and privacy systems will, from time to time, be compromised or otherwise become dysfunctional. Therefore, rather than demanding perfection, the law related to negligence and recklessness establishes a duty of care and determines whether a reasonable person would have acted as the defendant acted under the same circumstances. This is an extremely adaptive model, and can be readily applied to an infinite variety of circumstances that might be presented to the court in either a civil or criminal action. This negligence and recklessness model

---

172. Delaware is one the best known states engaging in race to the bottom induced by state-versus-state competition. *See* Mark J. Roe, *Delaware's Competition*, 117 HARV. L. REV. 588 (2003).

173. John R. Forbush, *Comment, Regulating the Use and Sharing of Energy Consumption Data: Assessing California's SB 1476 Smart Meter Privacy Statute*, 75 ALB. L. REV. 341 (2011-2012).

174. *See* Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards*, 25 YALE J. INT'L L. 1, 5-8 (2000). Of note is the manner in which the leadership of the European Union has enacted considerably stronger privacy laws and has thereby increased national standards since nations are blocked from doing business with the EU unless those standards are met. The U.S. federal government could do something similar to international standards of information security and privacy with a new negligence and recklessness law, such as the one found at the end of this article.

thus provides a legal model that is capable of dealing with unreasonably harmful conduct that is at this time and in the near future unknown.[175] The compliance-related regulatory and legal model mentioned above cannot deal with unknown future developments, although it is nonetheless a positive way to mandate those requirements that have been shown to be consistently beneficial, such as automobile seat belts. Again, here we see the need for a hybrid model going forward, a model involving both negligence and recklessness through risk assessment on one hand, and regulatory oversight plus contractual auditing[176] through compliance assessment on the other hand.

Perhaps the most compelling reason to rely more so on negligence and recklessness law than Americans do now is that the law evolves slowly, while information systems technology, in comparison, evolves rapidly. We now have a large divergence in the degree to which these two domains reflect the reality of today's contemporary society.[177] This divergence is becoming wider and increasingly problematic and appears to be a harbinger of increasingly costly and painful information security and privacy problems. Assuming that the law will not be able to catch or keep up with the pace of change in the information technology field, there must be a relinquishment of the faith in the current legal approach that places its primary reliance on laws and regulations that involve compliance, as described above. Instead, there should be greater emphasis on the development of a legal and regulatory process for handling information security and privacy that uses evidence-based feedback to determine what works and what does not (this feedback is, in turn, manifest in an industry specific standard of due care). Such an evidence-based process approach can be achieved through considerably greater reliance on the common law negligence and recklessness approach, as recommended by this article.

Still another argument for the dynamic nature of the negligence and recklessness-based model described in this article has to do with realistic modesty. Although many people are well-meaning and do have innovative proposals to improve information security and privacy through some new process or invention, history has shown that the vast majority of these proposals are soon obsolete, if not dysfunctional or forgotten. Accordingly, we should not empower these people to enact laws and regulations that mandate their own solutions—be they some new process for evaluating security and privacy or some new technology that supposedly will be a panacea. Instead, we should allow the marketplace of ideas to allow the most useful approaches to improving information security and privacy to

---

175. *See* Mark P. Gergen, *Negligent Misrepresentation as Contract,* 101 CALIF. L. REV. 953, 1007 (2013).

176. The Payment Card Industry Data Security Standard (PCI DSS) relies upon merchant compliance with security and privacy controls as a condition of providing continued payment related services. *See* PCI FAQs, PCI SECURITY STANDARDS COUNCIL, https://www.pcicomplianceguide.org/pci-faqs-2. Non-compliance with PCI DSS requirements is punished by fines and/or loss of payment related services, and those impacts serve as significant motivators to comply. Id. Non-compliant merchants may also be required to pay credit card replacement costs, foot the bill for forensic audit studies, and suffer damage to their brand from adverse publicity. *Id*. A comparable serious focus on motivational factors needs to be adopted in the area of existing federal law related to top management personal liability.

177. Andrea M. Matwyshyn, *Material Vulnerabilities: Data Privacy, Corporate Information Security, and Securities Regulation*, 3 BERKELEY BUS. L.J. 129 (2005).

prevail, without undue constraints. This approach, which in fact, is in keeping with "creative destruction"[178] capitalistic economic theory, can be supported by the increased reliance on the negligence and recklessness model advocated in this article.

XIII. CONCLUSION

The United States now has several decades of historical experience in the information security and privacy field, and that period's shockingly damaging experience clearly shows that Adam Smith's "invisible hand" of the marketplace is not adequately evolving the marketplace fast enough, or substantially enough, to successfully respond to the information security and privacy problems that plague the nation. Likewise, there is ample evidence that current top management incentive systems are not causing top managers to make the best decisions in this critical area. On the contrary, existing incentive systems such as quarterly bonuses, short-term stock options, and frequent inter-organizational job changes, encourage both underinvestment and inaction in the information security and privacy area. Such underinvestment and inaction can be traced directly to the decisions made by top management. These are the very people who are most influential in, and also who must be actively involved in, the resolution of this problem in order for it to be successfully solved. We must establish a new set of incentives that cause top management to act in ways that result in prudent, effective levels of information security and privacy.

Information security and privacy problems have reached a state of widespread crisis and emergency, and Congressional lawmaking intervention to establish a consistent nationwide federal solution is essential. But since much is at stake, considerable concern about unintended consequences and unexpected outcomes is warranted when undertaking any legal and regulatory intervention. This article proposes a politically palatable, and exceedingly conservative, minimal-level of intervention associated with a rebalancing of top management incentives and personal liability. The proposed way forward may be characterized as a reversion to a legal model where there was much greater reliance on the laws of negligence and recklessness than is currently seen in the American legal system. The ways in which the laws of negligence and reckless will be applied to information security and privacy issues must be clarified and adjusted. For example, modern defenses to negligence and recklessness—like the business judgment rule and the assumption of risk—need to be scaled back so that top management is strongly incentivized to look after the interests of third parties such as employees, customers, business partners, and members of the general public, not just the interests of shareholders and related constituencies. Detailing the way forward, this article has focused on risk management, and its suggested approach compliments, rather than replaces, existing compliance-related approaches to improving information security and

178. For the general theory of "creative destruction," *see* JOSEPH A. SCHUMPETER, CAPITALISM, SOCIALISM, AND DEMOCRACY (3d ed., Harper & Bros., 1950). New information technologies are provoking a wide variety of legal issues. In order to expeditiously respond to these information technology induced provocations, the law must be made more flexible. *See* Jack Wroldsen, *Creative Destructive Legal Conflict: Lawyers as Disruption Framers in Entrepreneurship,* 18 U. PA. J. BUS. L. 733 (2016).

privacy.

We now have the benefit of history to clearly understand cause and effect, what might happen, what is at stake, and what must be done. From a legal standpoint, that is sufficient to establish a standard of due care, what constitutes a breach of that standard, and whether the damage in question could have been foreseen. Thus, the existence of negligence and recklessness can now readily be determined by a court of law. A change in the law related to incentive systems for top management, a change that incorporates new definitions of negligence and recklessness, would go a long way to solving the information security and privacy problems with which America now wrestles. A Congressional research committee should be promptly established to investigate how a new national law similar to the one set forth in the appendix to this article might help restore faith, confidence, and trust in the information systems technological infrastructure, on which so much of modern American life is dependent. Congressional hearings to discuss such a law, or a conference of experts to discuss the merits of such a law, may also be appropriate next steps.

APPENDIX 1. DRAFT FEDERAL STATUTE:

Information Security and Privacy Top Management Negligence and Recklessness Act (the "Stewards of the Public Trust Act")

Legislative Intent: Information systems and related information networks have become pervasive and critical components of modern American society, components on which many different types of stakeholders now depend. National security, national competitiveness, and national welfare all now critically depend on effective and reasonable information security and privacy control measures. In response to these new conditions, a new top management stewardship responsibility toward the stakeholders other than shareholders has emerged. Acknowledging that there is a need for the legal recognition of this important position of stewardship, this Act recognizes both a criminal and a civil form of liability related to information security or privacy. These offenses occur when top managers fail to establish effective and reasonable control measures that protect information systems and/or information networks, in a manner consistent with the standard of due care for their particular industry.

Supersedes Existing Authorities: This Act applies to all organizations that come within the jurisdiction of federal courts, and according to the U.S. Constitution's Commerce Clause, this Act unifies all related legislation in all federal jurisdictions of the United States into this single statute. This Act, and all revisions subsequently passed by Congress and duly signed into law, supersedes all other statutes that directly address the subject matter of this Act. Thus, all state, city, county, or other government statutes, in addition to corporate charters, corporate articles, certificates of incorporation, corporate by-laws, not-for-profit organizing documents, trust creation documents, corporate contractual agreements with top management, insurance contracts, and related legal documents which either free and/or indemnify top management from personal liability, and/or limit top management personal liability exposure, for a breach of the duty of care, as discussed in this statue, are insofar as they conflict with any provision in this Act, henceforth both void and unenforceable on all the matters discussed in this Act.

Similarly, nothing in directors' and officers' insurance policies, employment contracts, corporate charters, or similar legal documents, as mentioned in the prior paragraph, shall prevent the assets of the organization in question from being used under the doctrine of vicarious liability or respondeat superior, to satisfy an adverse judgment rendered against one or more top managers under this Act. But such vicarious liability or respondeat superior responsibility applies only when the personal assets of the top managers judged to be liable have first been depleted in satisfaction of a judgment under this Act.

Offenses: Whoever, when acting in the capacity of a top manager in charge approving the budget that allocates resources for information security and/or information privacy, materially fails to establish effective and reasonable control measures that are consistent with the standard of due care employed by other organizations in the same industry, and such failure directly and proximately leads to a loss as defined in this Act, shall be guilty of or liable for either negligence or recklessness in the management of information security and/or privacy. A civil right

of action is hereby expressly recognized, as is a crime, and the latter is recognized as a felony. Civil rights of action may be brought under this Act as an individual plaintiff, as a joined group of plaintiffs, as a class action, and/or as a shareholder derivative suit involving one or more of the shareholders in the involved organization.

Duty of Care: Top manager defendants owe a duty of care, from both a negligence standpoint and a recklessness standpoint, to all third parties with whom they have an existing relationship, whether that relationship has been established by formal business contract or business-related circumstantial events. These third parties include, but are not limited to, business sales prospects, health care patients, product-purchasing customers, business partners, outsourcing firm staff, contractors, consultants, employees, persons described in a database maintained by top management's organization, and co-defendants in a lawsuit.

The duty owed to these third parties includes, but is not limited to, maintaining personally identifiable information provided by the third parties, and received by the organization that top management supervises, so that the information is kept in a secure and private manner, as is consistent with the prevailing standard of due care in the industry in question, or the equivalent standard of due care in government agencies or non-profit organizations. The nature of, and the limits related to, this same prevailing standard of due care, applicable to the industry involved, shall in all cases be established by testimony, written evidence, video statements offered, and the like issued by experts working in the field of information security and/or privacy.

Although not limited to the following four objectives, this duty requires top management to ensure that information provided by third parties is reasonably protected from (1) unauthorized usage, (2) unauthorized disclosure, (3) unauthorized modification, and (4) unavailability—any of which would cause material and serious harm to any of these third parties. This duty includes the requirement to reasonably notify third parties when information about them has been compromised in a manner that is likely to cause a material loss, if the third parties can reasonably do something in response to the notification to protect themselves. The duty also includes the requirement to correct materially incorrect information disseminated to these third parties about the status of information security and/or privacy at the organization that the top manager oversees. Furthermore, this duty requires that third parties be allowed to terminate their relationship with the organization that the top manager supervises without an unreasonably burdensome information security and/or privacy related penalty being imposed.

This duty to third parties furthermore includes maintaining the organization's own information systems, and assets (assets that are intellectual, informational, and/or physical in nature) controlled by these information systems, so that steps are taken to reasonably protect third parties from physical, financial, reputational, and/or informational harm. Where top management is the only party that can reasonably take such steps, or initiate such steps, so as to provide additional information security and/or privacy, this duty of care accrues, thereby requiring that top management take such steps if these steps are both reasonable and consistent with

the standard of due care industry practices mentioned above.

Negligence Per Se: No intention to cause harm, malice, or mens rea requirement is necessary in order to show a breach of the duty of due care in the area of information security and/or privacy. Plaintiffs need only show that the top manager defendant failed to engage an independent expert third party, who is free from material conflicts of interest on at least an annual basis, to review the information security and privacy status of a majority of the organization's units and prepare a detailed report of recommended improvements. That fact alone will establish negligence per se.

Standing: To establish standing to prosecute or sue, third party plaintiffs must have suffered demonstrable direct damages that in aggregate value total at least $75,000 (or must demonstrably be in imminent danger of suffering such harm when an injunction is involved). This threshold may be met by damages suffered by a specific plaintiff, a class of plaintiffs, or a successor in interest to either a specific plaintiff or a class of plaintiffs. In addition, to establish standing, these damages must have been actually and proximately caused by the top manager's failure to establish and maintain effective and reasonable control measures consistent with those used by other firms in the same industry as the organization in question.

Damages: To prove damages when there have been no monetary transactions to demonstrate the extent of those same damages, for example with privacy violations, courts shall, under this law, be authorized to establish damages as the cost to reestablish the status quo before the harm in question took place. The tort law doctrine known as the "economic loss rule" thus does not apply to this particular Act; in other words there does not need to be physical property damage or personal injury damage in order for damages to be recoverable under this Act.

Penalties:

(a) Criminal - The crime of negligent information security or privacy management is a Class A felony for which punishment, both imprisonment and fines, will be defined by federal sentencing guidelines. The court hearing a case involving negligent information security or privacy management may use its discretion to impose fines exceeding those found in the federal sentencing guidelines, up to a total of $100,000,000 per defendant, as equity may require.

The crime of negligent information security or privacy management is a strict liability offense, and no foreseeability is required to prove guilt under this Act. Guilt is established by an top manager's misfeasance, nonfeasance, failure to act, or willful blindness, such that a materially deficient information security or privacy control measures, i.e., control measures that diverged materially from an industry related standard of due care, prevailed at the time that the harms in question took place, and but for that state of control measures, the harms to person or property would not have taken place.

(b) Civil - A federal private right of action under the theory of negligence per se is expressly authorized hereby. Such a private right of action can impose direct personal liability on the involved top manager, regardless of whether the top manager was at the time acting in the capacity of an agent for the organization in question, if it can be shown that such a top manager made the budgetary decisions related to the information security and privacy control measures that prevailed at

the time of the plaintiff's loss. An information security and privacy management related duty of care is expressly established for top managers by this Act. A breach of that duty may be demonstrated by a failure to establish and maintain effective and reasonable information security or privacy control measures, such that the measures in existence materially diverged from the industry specific standard of due care. Actual cause may be established where the harm to person or property would not have been sustained, but for the failure of the top manager to establish and maintain effective and reasonable information security or privacy control measures consistent with an industry specific standard of due care.

Proximate cause for such an offense can be proven without a showing of the foreseeability of the specific risk that caused the harm in question. Thus the "extraordinary in hindsight" doctrine may be used to establish all manner of possible consequences that occurred because the top manager had materially failed to provide effective and reasonable information security or privacy. To establish dependent cause, it is sufficient to show that the risk of harm was materially enhanced by the top manager's failure to establish effective and reasonable information security or privacy control measures, consistent with the industry related standard of due care. Intervening dependent causes, such as a system attacker's actions, will not be considered a separate cause that diminishes the extent of the top manager's negligence under this Act.

(c) Punitive Damages - Treble compensatory damages (punitive damages) are authorized in those cases under this Act where the plaintiff makes a successful showing that the involved top manager was willful in his or her inattention to information security and/or privacy. Such willful intent may be established by any method that the court deems proper, but it will clearly be demonstrated by multiple unaddressed but serious reported incidents of information security or privacy losses taking place over the course of at least two months, or by the top manager's knowing refusal to allocate sufficient resources to improve information security and/or privacy so as to become compliant with minimum industry-related standard of due care. Thus, intention to harm specific people or property can be demonstrated by transferred intent. So where the defendant is shown to have been willful in his or her inattention to information security or privacy matters, that will be sufficient to show intent to harm others or their property.

Remedies: In addition to criminal fines, imprisonment, civil compensatory damages, and civil punitive damages, injunctions may issue upon the showing of sufficient cause. At the discretion of the court, attorney's fees, expert witness fees, court costs, and other actual and reasonable costs may be awarded to either the prosecuting government agency obtaining a conviction or the prevailing plaintiff.

Defenses: No scienter requirement is necessary for either a criminal conviction or civil liability with negligent information security or privacy management. Mere negligence is sufficient, and judgment does not depend on the level of knowledge that the top manager possessed. It is sufficient that such a top manager failed to exercise a duty of care that a reasonably prudent manager in the same industry would have employed, so as to provide effective and reasonable information security and privacy control measures consistent with industry standards of due care.

Both vicarious liability and respondeat superior are not recognized defenses to negligent information security or privacy management under this Act. While a top manager defendant is an agent of the organization for which he or she works, because a violation of a law would be a violation of an agent's duty of loyalty, the violation of this Act is deemed a personal frolic, and cannot be considered to be either within the scope of employment, or a detour from the scope of employment.

Statements in articles of incorporation, certificates of incorporation, by-laws, or similar official documents adopted by the corporation, as such a "corporation" is defined in this Act, shall not limit or eliminate the personal liability established by this Act. Nonetheless, directors and officers insurance, or other types of insurance, may be arranged by and paid for by the involved corporation to help pay the damages and other costs for which top managers are held personally liable under this Act. Nonetheless, if an action under this Act establishes that the defendant top manager knowingly chose to maintain ineffective and/or unreasonable control measures, that fact alone would be a breach of the duty of good faith, which includes the duty to observe and uphold laws such as this, and therefore the involved top manager would not be protected via such indemnification.

Safe Harbor: Top managers can fully and effectively defend and immunize themselves against all negligence and recklessness charges, both criminal and civil, as defined under this Act, by making a convincing showing to the court of all of the following three essential conditions: (1) the organization has adopted, and diligently employed, for over a year prior to the time when the damages in question were sustained, a formal documented risk management system to bring information security and privacy problems to top management's attention, to diligently manage progress on projects in this same area, and to reveal the current organizational state of information security and privacy, (2) the organization has routinely employed independent third party professional experts in the domain of information security and privacy, to make organization-wide assessments, of all material risks and related control measures, on at least an annual basis, for all of the past three years, and (3) the top manager defendant has not been placed on notice, about any material deficiencies in the information security and privacy area, by such a professional expert over the prior twelve-month period leading up to the time when the damages in question were sustained.

Another way that such safe harbor may be obtained is via a due diligence defense. In order to successfully plead such a defense, the defendant must make a convincing showing of all three of the following conditions: (1) the organization has adopted, and diligently employed, for over a year prior to the time when the damages in question were sustained, a formal documented risk management system to bring information security and privacy problems to top management's attention, to manage projects in this same area, and to reveal the current organizational state of information security and privacy, (2) the organization has routinely employed independent third party professional experts in the domain of information security and privacy, to make organization-wide assessments, of all material risks and related control measures, on at least an annual basis, for all of the past three years, and (3) even though the top manager has been placed on notice of one or more material deficiencies by such a professional expert, a credible and reasonable process of expedited remediation addressing these deficiencies can be demonstrated

by specific management acts, specific documents issued, changes in information systems, or other convincing dated evidence, and such a remediation process was both established and operational for at least six months prior to the time that the loss in question took place.

Potential Defendants: As used in this Act, the term "top manager" includes all executive managers in traditional corporations and also in new entity types such as limited liability corporations and limited liability partnerships. It additionally includes top managers at traditional partnerships, non-profit organizations, charities, non-governmental-organizations, foundations, and government agencies at all levels of government. Defendant top managers subject to liability via this Act are only those managers who are personally responsible for approving the information security and privacy budget. Those top managers who are potential defendants under this Act may have a wide variety of titles such as Chief Executive Officer, Chief Information Officer, or Chief Operations Officer, and their obligations under this Act stem entirely from their formally-designated duties related to budget approval. These same obligations are not determined by job title, nor are they determined by status as a legal officer of the organization.

Exempt Organizations: This Act does not apply to top managers at organizations that have never reached either $10,000,000 or more in either sales or donations, or 10,000 or more customers or users. Managers at organizations that do not meet either of those two thresholds are exempt from all provisions of this Act. All top managers as described in this Act who are working in government agencies are subject to this Act, and to them, the thresholds in this paragraph do not apply.

Business Judgment Rule Defense: The business judgment rule defense shall not apply to matters addressed in this Act unless the defendant can clearly and convincingly demonstrate to the court all of the following: (1) one or more independent third party experts in the field of information security and privacy were retained by plaintiff's organization at least one year before the date of the first event in the complaint filed by plaintiff or prosecutor, (2) the findings in the report issued by such a third party expert were diligently investigated, pursued, analyzed and employed to improve information security and privacy at the organization in question, for a period of at least one year prior to the first of the events on which the plaintiff or prosecutor is basing a claim, (3) after revealing the mechanism of action for all incentive systems applicable to the defendant at the time of the events described in that complaint, no material conflicts of interest existed, that would be likely to cause the defendant to act in a way that would be contrary to maintaining and supporting an adequate level of information security and privacy at the organization in question (as defined by standard industry practices), and (4) the information security and privacy measures in question demonstrably met or exceeded the industry related standard of due care for the organization in question.

Affirmative Defense of License: For purposes of determining negligence or recklessness under this Act, the affirmative defense of license, alleging that the defendant had contractual agreement with the plaintiff, or with the plaintiff's organization, allowing the conduct described in the plaintiff's complaint, can be recognized by the court only if all of the following four conditions apply. To employ this defense defendant must show that: (1) there was a valid existing

contract between the plaintiff and the organization that employed the defendant, (2) the plaintiff was aware, in all material respects, of the information security and privacy risks associated with entering into such a contract, (3) the contract was not one of adhesion, in other words there was a genuine "meeting of the minds" between the plaintiff and a representative of the organization that employs the defendant, and each such party was represented by counsel at the time that the contract was negotiated, and (4) such a contract does not expressly address, restrict, or limit the negligence or recklessness of the defendant, only that of the organization for which the defendant works.

Affirmative Defense of Assumption of the Risk: For purposes of determining negligence or recklessness under this Act, defendants will only be able to employ the assumption of risk defense if they can show that: (1) the plaintiff had a reasonable level of actual knowledge of relevant risks, that would enable plaintiff to make a reasonably informed decision, (2) plaintiff expressly and voluntarily agreed to assume the risk after obtaining such knowledge, and (3) the loss in question took place subsequent to the time that the plaintiff allegedly assumed the risk.

Waivers and Releases: Contractual waivers of rights, liability releases, and other agreements dealing with limitations on the right to sue under this law, the allocation of liability under this law, and/or the mandated arbitration of claims under this law, shall be void and unenforceable unless defendant can show that: (1) plaintiff had a reasonable level of actual knowledge about the relevant information security and privacy risks, and (2) comprehensible information about these risks had been provided to plaintiff before such a waiver, release, or other agreement was entered into by plaintiff. General disclosures found in contracts of adhesion, non-negotiable standard form contracts, legal disclosure forms, or Internet-based terms of service screens, do not suffice when it comes to providing the plaintiff with a reasonable level of actual knowledge so that the assumption of risk defense may be successfully claimed by the defendant. To employ this defense successfully, a defendant's disclosure of information about relevant risks must have been at a level of detail so that the plaintiff can reasonably understand both the nature of adverse future consequences associated with entering into an agreement regarding the assumption of risk, and the potential magnitude of such future consequences.

Contributory Negligence Defense: Contributory negligence and contributory fault, will not be recognized as a defense under this Act if the plaintiff was not actually and reasonably aware of the relevant risks involved at the time that the harm was suffered and so could not adequately guard against the possibility of adverse consequences resulting from assuming those risks. If, however, the plaintiff used a product or service, offered by an organization managed by the defendant, and that usage was in clear and explicit opposition to its ordinarily offered usage, or in opposition to clear and explicit instructions provided by the defendant's organization, then contributory negligence may successfully be employed as a defense. The use of the contributory negligence defense, as it relates to this Act, shall furthermore be restricted so that it can only be employed to the extent that plaintiff clearly and negligently assumed the risk out of all proportion to the interest to be obtained thereby.

Self-Executing: Upon passage by the Congress and the subsequent signing into

law by the President or by Congress's action to override the President's veto, this law shall be immediately effective and without need for any implementing action. No regulations need to be written, and no other governing body needs to adopt or approve this law in order for it to go into effect.

APPENDIX 2. KEY PROVISIONS OF THE PROPOSED NEW LAW CREATING A SOCIALLY-BENEFICIAL TOP MANAGEMENT INCENTIVE SYSTEM RELATED TO INFORMATION SECURITY AND PRIVACY:

(1) Require that organizations meet a minimum **industry-based standard of due care** related to information security and privacy in order for top management to be protected from personal liability related to negligence or recklessness, either civil or criminal in nature, in those cases where serious harm can be shown to have been caused to third parties,

(2) Eliminate the need to show **intention** to cause harm, malice, mens rea, and the like, in that negligence and/or recklessness can be clearly established in a straightforward fashion, via the per se doctrine, simply because an organization materially failed to meet an industry-related standard of due care in the information security and privacy area (and such a standard can be established by existing regulations and/or laws such as the Health Insurance Portability and Accountability Act),

(3) Create a straight forward and clearly delineated "**safe harbor**" process, involving the use of external expert consultants in the information security and privacy field (acting much like Certified Public Accountants in the Financial Reporting Act), which will be used to independently determine whether a firm has met the minimum standard of due care in a particular industry,

(4) Scale back the applicability of the **business judgment rule** that often inappropriately protects top management from being incentivized by negligence or recklessness lawsuits in information security and privacy harm to third party cases because the assumptions on which this rule is based are not relevant in the information security and privacy area,

(5) Strongly limit the use of **additional defenses**, such as acceptance of the risk defenses that may otherwise limit top management personal liability in information security and privacy cases so that these defenses more accurately reflect modern real-world conditions, including the fact that top managers are now often stewards of the public trust,

(6) Replace corporate charters, bylaws, executive employment contracts, waivers, releases, and other **legal agreements** that limit top management personal liability in the information security and privacy area with this new national law so that top management will always have a widely-understood standardized level of exposure to negligence and recklessness related personal liability, thus motivating adequate funding for, and attention to, both information security and privacy, and

(7) Permit **indemnification** to pay for information security and privacy harms suffered by third parties if such harms were caused by the negligence or recklessness of top management, but to maintain a truly effective incentive system,

allow such indemnification to be employed only after all the personal assets of liable top manager(s) have first been used to satisfy all judgments rendered under this statute.