Revista de Derecho Privado
E-ISSN: 1909-7794
mv.pena235@uniandes.edu.co
Universidad de Los Andes
Colombia

Rodríguez Parra, César Felipe
SEGURIDAD DE LA INFORMACIÓN: ESTRATEGIA PARA FORTALECER EL GOBIERNO CORPORATIVO
Revista de Derecho Privado, núm. 43, junio, 2010, pp. 3-24
Universidad de Los Andes
Bogotá, Colombia

SEGURIDAD DE LA INFORMACIÓN: ESTRATEGIA PARA FORTALECER EL GOBIERNO CORPORATIVO

*César Felipe Rodríguez Parra**

Resumen

Considerando que la Seguridad de la Información no puede existir sin un buen Gobierno Corporativo y viceversa, este documento tiene como objetivo integrar estos dos conceptos. El documento explora la creciente importancia de la información en el aseguramiento del crecimiento sostenible de las empresas y el evolutivo riesgo que aquella enfrenta, para proponer los principios de Gobierno Corporativo como una manera eficiente en la mejora de la seguridad y, por ende, en la activación de negocios sin comprometer la continuidad de las compañías.

Palabras Clave

Términos Clave: Gobierno Corporativo, Seguridad de la Información, Obligación Legal de Proveer Seguridad de la Información, Manejo del Riesgo, Revelación.

Abstract

Considering that Information Security cannot exist without good Corporate Governance and vice versa, this paper aims to integrate both concepts. The document explores the increasing importance of information in ensuring company sustainable growth and the evolving risk it faces in order to propose corporate governance principles as an effective way to improve security and, hence, enable businesses without compromising company's survival.

Key-words

Corporate Governance, Information Security, Legal Obligation to Provide Information Security, Risk Assessment, Disclosure.

* César Felipe Rodríguez Parra – Biography

Lawyer graduated from the Universidad de los Andes (Bogota). He studied a postgraduate course in Financial Law in the Universidad de los Andes (Bogota) and another in Civil Procedural Law of Universidad Externado de Colombia (Bogota). He is LL.M in International Business Law of The University of Liverpool (England). He has practiced law at ExxonMobil, KPMG and the law firm Prieto & Carrizosa, Attorneys at Law and he is author of the articles "Electronic Documents as Key Evidence in Commercial Lawsuits" and "Credit Default Swaps and international financial crisis". The author may be contacted at cesarf.rodriguez@gmail.com

César Felipe Rodríguez Parra – Biografía

Abogado graduado de la Universidad de los Andes (Bogotá). Especialista en Legislación Financiera de la Universidad de los Andes (Bogotá). Especialista en Derecho Procesal Civil de la Universidad Externado de Colombia (Bogotá). Master en Derecho de los Negocios Internacionales de la Universidad de Liverpool (Inglaterra). Ha ejercido como abogado en ExxonMobil, KPMG y en la firma de Abogados Prieto & Carrizosa. Dentro de sus publicaciones se cuentan los artículos "Documentos Electrónicos como Pruebas Claves en Litigios Empresariales" y "Credit Default Swaps y crisis financiera internacional". El autor puede ser contactado en cesarf.rodriguez@gmail.com

INTRODUCCIÓN

Debido a la innegable importancia legal y económica de la información para las compañías y el riesgo que éste activo enfrenta en la economía interconectada, los objetivos del Gobierno Corporativo (asegurar un crecimiento económico sostenible y mejorar la confianza del público en los mercados) no pueden ser cumplidos sin proteger la información de la pérdida, de la alteración no autorizada y de la revelación inapropiada.

No obstante, la Seguridad de la Información ha figurado muy poco en los debates sobre Gobierno Corporativo porque: (i) a pesar de existir algunas tendencias positivas, las Juntas Directivas no ven un caso de negocios en la Seguridad de la Información; (ii) los abogados corporativos usan la Teoría de Agencia para entender el Gobierno Corporativo, lo cual lleva a los comentaristas a concentrarse en las estructuras para la toma de decisiones y mecanismos de responsabilidad; y (iii) el personal del Departamento de Tecnología de las compañías sigue considerando la Seguridad de la Información como un simple asunto técnico y no como uno gerencial. Como consecuencia de esto, la Seguridad de la Información es asumida de manera desarticulada, al ser observada como un simple tema de cumplimiento legal o un simple problema técnico. Esto, a su vez, impide una efectiva administración de la Seguridad de la Información y compromete el logro de los objetivos del Gobierno Corporativo.

Elevar la Seguridad de la Información al nivel de un tema clave de Gobierno Corporativo contribuye al cumplimiento de los objetivos de éste último debido a que el compromiso de la Junta Directiva y de la alta gerencia permite una respuesta alineada y estratégica de varias funciones de la compañía (comercial, jurídica y tecnología de la información) y, adicionalmente, produce beneficios como ventajas competitivas y una mejor responsabilidad corporativa.

Tomando en cuenta la relevancia de la información, los riesgos a los que está expuesta y el interés del público en la Seguridad de la Información, la aplicación de los principios de Gobierno Corporativo de Revelación y de Manejo del Riesgo es fundamental para incluir la Seguridad de la Información en el alcance del Gobierno Corporativo.

Con el objeto de desarrollar el argumento, el presente documento tendrá la siguiente estructura: la Sección 2 describe la definición, objetivos y principios del Gobierno Corporativo. La Sección 3 establece la definición y objetivos de la Seguridad de la Información, así como su relevancia corporativa. La Sección 4 analiza la relación actual entre Gobierno Corporativo y Seguridad de la información. Para esto, primero se argumenta que la Seguridad de la Información actualmente no se encuentra en el alcance del Gobierno Corporativo y luego se exponen los efectos de tal desconexión, en particular, los efectos negativos que una débil Seguridad de la Información tiene en el logro de los objetivos del Gobierno Corporativo. La Sección 5 identifica las razones para incorporar la Seguridad de la Información en las estrategias de gobierno y muestra la aplicación de los principios de Revelación y Manejo del Riesgo como un método para incorporar la Seguridad de la Información en el Gobierno Corporativo de las compañías. Finalmente, la Sección 6 presenta las conclusiones del trabajo.

1. EL PANORAMA DEL GOBIERNO CORPORATIVO

Las definiciones de Gobierno Corporativo varían ampliamente. Bajo una definición restringida, el Gobierno Corporativo es una herramienta para crear una cultura administrativa que permite ofrecer participaciones accionarias para el público en general. Esto puede incluir requerimientos para listar una compañía en las bolsas de valores y reglas sobre revelación de información relevante para los inversionistas. Bajo una definición más enfadada a la provisión de financiamiento, el énfasis radica en la manera en que los inversionistas de capital se protegen frente a las decisiones de los administradores. Esto puede incluir la protección de los accionistas

minoritarios, el fortalecimiento de los derechos de los acreedores, la composición de las Juntas Directivas así como de sus facultades y la creación de procedimientos judiciales disponibles para los accionistas[1]. El Gobierno Corporativo también puede ser visto como una estrategia con objetivos medibles en la práctica, por ejemplo, mecanismos y procedimientos para hacer que la administración sea responsable de sus actos[2]. Desde una perspectiva económica, el Gobierno Corporativo consiste en una serie de reglas que crean condiciones para un comportamiento racional de negociación. Esta definición se refiere tanto a la determinación del valor agregado de las firmas, como a su distribución entre todas las partes interesadas (o *'stakeholders'*)[3].

En cualquier caso, un sólido gobierno es la base para el éxito empresarial de largo plazo. En términos exclusivamente financieros, los administradores deben incrementar las utilidades de la compañía para multiplicar la inversión de los accionistas[4]. Sin embargo, una aproximación más comprehensiva (*conocida como Stakeholder Theory*) considera los objetivos del Gobierno Corporativo como el crecimiento sostenible por medio de la supervivencia de las compañías y el mejoramiento de la confianza del público en el mercado[5]. Por ejemplo, la Organización para la Cooperación y Desarrollo Económicos (OECD) define Gobierno Corporativo como "un elemento clave en el mejoramiento de la eficiencia económica y el crecimiento, así como, el incremento en la confianza de los inversionistas"[6]. Sin olvidar la trascendental importancia de mantener y aumentar el valor para los accionistas, la *Stakeholder Theory* tiene en cuenta un grupo más amplio de interesados (empleados, prestamistas, clientes, proveedores, gobierno y la comunidad local) o *'stakeholders'* que deben beneficiarse de las actividades de la empresa[7]. Basada en la dependencia del mundo en las corporaciones por la variedad de funciones sociales que desarrollan más allá de los típicos roles de producción y empleo[8], la *Stakeholder Theory* considera el comportamiento real de las empresas en términos de desempeño, eficiencia, crecimiento, estructura financiera, y tratamiento de los accionistas y otros *stakeholders*[9].

Ahora bien, el Gobierno Corporativo está basado en una serie de principios. Por ejemplo, los principios de Gobierno Corporativo de la OECD (Principios OECD) son el resultado de consultar a los gobiernos de sus Estados Miembro, al sector privado y a varias organizaciones internaciones, lo que los convierte en elementos claves de buen Gobierno Corporativo reconocidos e incorporados por diferentes países[10]. Estos principios cubren seis áreas de Gobierno Corporativo, desde la promoción de mercados transparentes y eficientes, hasta el aseguramiento de una guía estratégica de la compañía[11]. Entre esos principios, la Revelación de información relevante y la obligación de la Junta Directiva de conducir la política de Manejo del Riesgo son principios fundamentales para integrar la Seguridad de la Información y el Gobierno Corporativo.

1 Shleifer, Andrei, and Vishny, Robert (1997), "A Survey of Corporate Governance", Journal of Finance, 52(2):737–83. p.737

2 Cadbury Committee (Committee on the Financial Aspects of Corporate Governance) (1992), "The Report of the Committee on the Financial Aspects of Corporate Governance", London.

3 Claessens, Stijn (2006), "Corporate Governance and Development", Oxford University Press, p.5

4 The Information Assurance Advisory Council (2002), "Engaging the Board: Corporate Governance and Information Risk", p.15

5 Salacuse, Jeswald (2004), "Corporate Governance in the New Century", Comp. Law. 2004, 25(3), p.70

6 OECD (2004), "Principles of Corporate Governance", p.11.

7 Mallin, Chistine (2007), Corporate Governance, Second Edition, Oxford, p.16.

8 Harshbarger, Scott and Jois, Goutam (2007), "Looking Back and Looking Forward: Sarbanes-Oxley and The Future of Corporate Governance", 40 Akron L. Rev. 1, p.1.

9 Claessens, Stijn, op. cit., p.3

10 Mallin, Chistine, op. cit., p.31-33

11 OECD (2004), "The OECD Principles of Corporate Governance. Policy Brief", p.2

2. EL PANORAMA DE LA SEGURIDAD DE LA INFORMACIÓN

Antes de continuar con la discusión, es necesario entender la relevancia de la Seguridad de la Información, la cual constituye la justificación para elevarla como un tema de Gobierno Corporativo. Por lo tanto, esta Sección define Seguridad de la Información, expone las amenazas que pretende combatir y, finalmente, explica las razones por la cuales se debe considerar la Seguridad de la Información como un asunto corporativo crítico.

2.1 Definición y amenazas de la seguridad de la información

La Seguridad de la Información es el proceso de proteger la información de la pérdida, de la alteración no autorizada y de la divulgación inapropiada. Los objetivos de la Seguridad de la Información son, entonces, la confidencialidad, la integridad y la disponibilidad de la información. La confidencialidad consiste en mantener la información fuera del conocimiento de personas que no están autorizadas para acceder a ella. La integridad asegura que la información permanezca inalterada y completa. Finalmente, la disponibilidad se refiere a que la información y los sistemas de comunicación permanezcan accesibles para sus usuarios oportunamente[12].

Esos objetivos son seriamente amenazados en la economía interconectada. La digitalización de la información y la interconexión de las redes corporativas con Internet representan ventajas en la manera en la cual se adelantan negocios, porque los computadores y las redes hacen más eficiente el uso de la información y, en consecuencia, incrementan la productividad, permitiendo coordinar múltiples procesos de negocio[13]. Sin embargo, esos desarrollos tecnológicos también crean nuevas amenazas que las compañías tienen que sortear. En términos generales, tales amenazas son: (i) códigos maliciosos; (ii) ataques de negación de servicio (*Denial of Service Attacks o DoS*); y (iii) suplantación de identidad.

Los códigos maliciosos (virus, *worms* y troyanos) básicamente destruyen o alteran los archivos electrónicos. Un virus es un programa cargado en un computador sin el conocimiento del propietario, que realiza acciones que él no ha autorizado. Un virus es capaz de replicarse y activarse por sí mismo. Los virus pueden infectar diferentes partes de un sistema informático, dañar los archivos electrónicos o tan sólo mostrar su presencia. Por otra parte, un worm es un programa de computador, que usa una red para enviar copias de su mismo a otros computadores o redes sin la intervención del usuario. Por último, un troyano necesita que el usuario los instale y ejecute, y puede causar cualquier efecto indeseable, por ejemplo, la destrucción de los archivos y proveer medios para que otros computadores violen los controles de acceso[14]. . Debido a los códigos maliciosos, la integridad de la información almacenada en el sistema infectado es seriamente comprometida, con altos costos financieros. Por ejemplo, el *worm* Código Rojo (*Code Red worm*) causó cerca de 2.6 billones de dólares en pérdidas, mientras que el virus Klez 9 billones de dólares[15].

Por su parte, los DoS son un intento de deshabilitar un recurso informático. En su forma más simple, los DoS buscan denegar acceso a los usuarios de los computadores sobrecargando el objetivo (un computador, un servidor o una red) con comunicaciones indeseadas. Una forma más sofisticada de este tipo de ataque utiliza redes de computadores comprometidos (conocidos como

12 Koops (1999), The Crypto Controversy, A Key Conflict in the Information Society, Kluwer Law International.

13 Atrostic, B.K. and Sang, Nguyen (2006), "How Businesses Use Information Technology: Insights for Measuring Technology And Productivity", CES 06-15, 2006

14 Symantec Internet Security Threat Report (March 2007), Volume XI

15 See: <http://www.isn.ethz.ch/edu/adl/standalone_obj/Sec_Inf_Age/scos/2/index.html>, última visita Agosto 30, 2007.

'robots' o 'zombis') para bombardear el objetivo con una enorme cantidad de información[16]. A pesar de cierta discusión al respecto, los riesgos comerciales asociados con los DoS pueden ser elevados[17]. A parte de los costos de remediación y el impacto en la reputación, las víctimas enfrentan costos adicionales en software y consultoría junto con el riesgo de pagar mayores tarifas de conexión a la red. Por ejemplo, en el caso Lennon[18], el acusado atacó a la red de su anterior empleador con un software que enviaba masivamente correos electrónicos, reportando un costo de 30.000 libras sólo en pérdidas de negocios[19].

Finalmente, la suplantación de identidad está emergiendo como uno de los crímenes más serios del siglo XXI[20]. De acuerdo con la Encuesta Global de Seguridad realizada por Deloitte en (*2006 Global Security Survey*), la suplantación de identidad es una de las prioridades de las instituciones financieras[21]. Este tipo de ataques involucra una sustracción deliberada de la información de otra persona obteniendo sus contraseñas y usando la falsa identidad para violar la seguridad de ciertos sistemas. Esa información puede ser luego utilizada para cometer otro delito, usualmente fraude[22]. En el caso Monster.com, hackers sustrajeron datos de dicha página web con el objetivo de obtener información mucho más valiosa que sólo nombres y detalles de contacto de los usuarios de Monster.com. Haciéndose pasar por empleadores, los hackers enviaron correos electrónicos que solicitaban a sus receptores proveer información financiera, como números de cuentas bancarias. El objetivo final de irrumpir en Monster.com fue obtener suficiente información personal para disminuir las defensas de las posibles víctimas cuando ellos leyeran los correos electrónicos[23].

2.2 La relevancia corporativa de la seguridad de la información

La Seguridad de la Información tiene una significativa relevancia corporativa porque tiene como objetivo proteger un activo extremadamente importante y porque existe una amplia regulación que obliga a las compañías a proveer Seguridad de la Información.

2.2.1 Importancia de la información

En el pasado, cualquier gerente al que le preguntaras sobre el activo clave de su negocio, muy probablemente hubiera contestado que tal activo eran sus productos o óbrale recurso humano. En la actualidad, más y más negocios están reconociendo que uno de sus activos más valiosos es la información. Sin importar que la información sean bases de datos de clientes, know-how o registros contables, la habilidad de almacenarla, recuperarla y manipularla de manera segura es crucial para el éxito en los negocios. Esta situación se ha vuelto aún más evidente desde que el 80 por ciento de los activos corporativos son digitales[24].

16 CERT Coordination Center (October 2001), "Trends in Denial of Service Attack Technology", disponible en: <www.cert.org/archive/pdf/DoS_trends.pdf>, última visita Agosto 30, 2007.

17 Esta discusión se considera en la Sección 4.2.1.

18 R v. Lennon, Judgment of District Judge Kenneth Grant, Youth Court in Wimbledon, November, 2005.

19 Worthy, John (2007), "Denial-of-Service: Plugging the Legal Loopholes?", CLSR 2 3, p.194

20 Siegel, Kenneth (2007), "Protecting The Most Valuable Corporate Asset: Electronic Data, Identity Theft, Personal Information, and The Role of Data Security in The Information Age", 111 Penn St. L. Rev. 779, p.781

21 Deloitte, "Global Security Survey 2006", p.13

22 Kendrick, Rupert (2002), "Cyber-risks—How are You Managing Them?", 152 NLJ 7053.

23 Reuters, "Monster.com Took 5 Days to Disclose Data Theft", disponible en: <http://www.reuters.com/article/technologyNews/idUSWNAS278320070824>, última visita noviembre 29, 2009.

24 Siegel, Kenneth, op. cit., p.779

La información es valiosa debido a tres razones. En primer lugar, cierta información representa intrínsecamente dinero, por ejemplo, la propiedad intelectual. En segundo término, la información es la materia prima para tomar decisiones, un activador de negocios sin el cual muchas organizaciones simplemente no podrían funcionar[25]. Por ejemplo, estudios relacionados con un nuevo campo petrolero representan el principal criterio de decisión para que una compañía petrolera inicie un nuevo proyecto de exploración. Si esa información sufre cualquier daño, la compañía podría invertir una enorme cantidad de dinero en un proyecto equivocado o podría perder una excelente oportunidad de negocios. Por último, la confiabilidad de la información en línea es un prerrequisito de la expansión del comercio electrónico. El comercio electrónico implica un intercambio de información con personas desconocidas situadas a bastas distancias, lo cual crea un complejo problema de confianza[26]. Los negocios electrónicos (e-business) no pueden ser exitosos si el público y la compañía misma no pueden estar seguros que el sistema informático de la compañía es confiable y que la información está segura[27]. La falta de confianza en la autenticidad de la información crea una incertidumbre legal, por lo tanto, las compañías que no pueden confiar en sus sistemas de información y comunicaciones dudarán en usar las nuevas tecnologías para adelantar transacciones.

2.2.2Obligación legal de proveer seguridad de la información

La obligación de las empresas de garantizar Seguridad de la Información no se encuentra en un cuerpo normativo unificado, al contrario, dicha obligación se encuentra en legislaciones que regulan otros temas, por ejemplo, legislación sobre protección de datos personales y sobre Gobierno Corporativo.

Las leyes sobre protección de datos personales es la respuesta legal a la habilidad de las compañías de recolectar y transmitir grandes cantidades de información personal, es decir, información que permita identificar directa o indirectamente a una persona. Esta situación ha creado temas de privacidad y ha llevado a varias jurisdicciones en todo el mundo a promulgar leyes con el objetivo de proteger la información personal, las cuales normalmente incluyen provisiones sobre seguridad como complemento a su objetivo de asegurar la privacidad de las personas[28].

En los Estados Unidos, en lugar de tener una ley general sobre la protección de datos personales que aplique en todas las industrias, los legisladores norteamericanos han optado por crear provisiones especiales para cierto tipo de datos personales, tales como información financiera o registros médicos. Esas leyes generalmente establecen requerimientos generales en relación con la recolección y uso de la información relevante para el ámbito al cual aplican[29]. Por ejemplo, la ley *Gramm-Leach-Billey*[30] (Ley GLB) contiene provisiones en relación con la privacidad de la información de los clientes de las instituciones financieras. Básicamente, la Ley GLB restringe la habilidad de las instituciones financieras para revelar la información financiera de un cliente a otra sociedad que no hace parte del grupo bancario y obliga a las instituciones financieras a proveer notificaciones acerca de las prácticas de recolección y circulación de la

25 IT Governance Institute (2006), Information Security Governance, Guidance of Boards of Directors and Executive Management, Second Edition, P.12

26 Purser, Steven (2004), *A Practical Guide to Managing Information Security*, Artech House, p.14-15

27 Siegel, Kenneth, op. cit., p.779

28 Klosek, Jacqueline (2005), *"Corporate Legal Departments, Third Edition"*, Practising Law Institute, Appendix A16. Privacy and Data Protection Law.

29 Ibid.

30 Pub. L. No. 106-102, 15 U.S.C

31 Klosek, Jacqueline (2005), op. cit.

información de sus clientes[31]. En relación con las provisiones de seguridad, la Ley GLB requiere a la Comisión Federal de Comercio (Federal Trade Comission o FTC) la creación de estándares que las instituciones financieras deben cumplir para proteger la información personal de sus clientes. Bajo este requerimiento fue promulgada la Regla de Salvaguardias de la FTC (FTC Safeguards Rule) que representa la articulación más comprensiva de este organismo en relación con a la seguridad de los datos personales. El objetivo primordial de esta regulación es la implementación de un programa de Seguridad de la Información que sea apropiado al tamaño y naturaleza de la organización, al alcance de sus actividades y a la importancia de la información que está en juego[32].

Por otra parte, la pieza clave de la legislación europea en este tema es la Directiva sobre Protección de Datos Personales[33] (*Data Protection Directive*) que actúa como una serie de indicaciones para los Estados de la Unión Europea, requiriéndolos para que implementen ciertas provisiones en sus leyes nacionales[34]. La Directiva establece una regla relativamente amplia y general en relación con la seguridad de los datos personales[35]. El Artículo 17(1) dispone: "Los Estados miembros establecerán la obligación del responsable del tratamiento de aplicar las medidas técnicas y organización adecuadas, para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados, en particular cuando el tratamiento incluya la transmisión de datos dentro de una red, y contra cualquier otro tratamiento ilícito de datos personales"[36]. Adicionalmente, en la determinación de las medidas de seguridad que podrían ser apropiadas, la Directiva solicita a los responsables de los datos considerar el estado del arte en el que se encuentre la tecnología, el costo de la implementación de las medidas de seguridad, así como, los riesgos representados por el procesamiento y la naturaleza de los datos a ser protegidos[37]. Un ejemplo de normatividad nacional que sigue los parámetros señalados por la Directiva Europea es la Ley británica de Protección de Datos Personales[38] (Data Protection Act o DPA), la cual gira en torno a ciertos principios que los controladores de datos deben cumplir para proteger los datos personales[39]. En particular, el séptimo principio del DPA se encarga de los temas de la seguridad de los datos personales. El séptimo principio y su interpretación[40] proveen las medidas técnicas y organizacionales que deben ser tomadas en contra del procesamiento ilegítimo o no autorizado de la información personal, así como, de su pérdida, destrucción o daño[41].

La obligación de proveer Seguridad de la Información dentro de las compañías también se puede encontrar en las leyes conocidas como de Gobierno Corporativo. Esas regulaciones no sólo están encaminadas a asegurar que la contabilidad sea llevada de manera apropiada, sino también a asegurar que los directores cumplan apropiadamente todos sus roles, incluyendo el cuidado de los activos corporativos. Los administradores deben asegurarse de cumplir con sus deberes y obligaciones, tomando especial cuidado respecto a sus sistemas de información[42].

32 Colbath, Bruce (2006), "Customer Privacy and Data Security: The Importance of Guarding Your Henhouse", *60 Consumer Fin. L.Q. Rep. 603, p. 605*

33 Council Directive No. 95/46/EC of 24 October 1995 on the Protection of Individuals with Regard to the Processing of personal data and on the Free Movement of Such Data, O.J. L 281/31 (1995).

34 Klosek, Jacqueline (2005), op. cit.

35 Ibid.

36 Council Directive No. 95/46/EC, art. 17(1).

37 *Ibid.*, art. 17(2).

38 Data Protection Act 1998.

39 Reed, Chris and Angel, John (2007), Computer Law, Oxford, Sixth Edition, p.477

40 Data Protection Act 1998. Part I. Principle 7 and Part II. 9-12

41 Baker, Catherine (2000), "New Data Protection Act", *Ent. L.R. 2000, 11(8),* 193-196, p.195

42 Information Assurance Advisory Council (2002), op. cit., p.5.

El ejemplo más notable de este tipo de legislación es la Ley Sarbanes-Oxley[43] (*Sarbanes-Oxley Act* o SOX). A pesar de que el principal objetivo de SOX es restaurar la confianza en los mercados públicos[44], ésta ley contiene dos secciones relevantes para la Seguridad de la Información. La sección 404 requiere al presidente de la compañía (*Chief Executive Officer o* CEO) y al Vicepresidente Financiero (*Chief Financial Officer o* CFO) de una compañía que cotiza en bolsa, cuando firman los estados financieros de la compañía, certifiquen que la sociedad cuenta con adecuados sistemas de control interno sobre su información[45]. La sección 302 preceptúa que, en adición a certificar la precisión de los registros divulgados, los administradores tienen que asegurar que son responsables por el control interno, han designado tales controles para asegurar que la información relevante ha sido puesta a su consideración, han evaluado y reportado la efectividad de esos controles y han discutido en el reporte cualquier cambio en el control interno[46]. El cumplimiento de SOX ha llevado a crear consciencia sobre control interno, auditoría y Seguridad de la Información, lo cual no sólo ha sido usado como una herramienta para obtener un buen Gobierno Corporativo y controles financieros, sino también para ver a la Seguridad de la Información como un objetivo en sí mismo, ya que cualquier incidente de seguridad puede causar fácilmente una imprecisión en los sistemas de reporte financieros de las compañías[47].

43 Public Company Accounting Reform and Investor Protection (Sarbanes-Oxley) Act of 2002, Pub. L. No. 107-204, 116 Stat. 745

44 Hewlett-Packard (2006), "Sarbanes-Oxley and the IT organization: A Survival Guide", p.3

45 Schwartz, Paul and Janger, Edward (2007), "Notification of Data Security Breaches", 105 Mich. L. Rev. 913, p.924

46 Langevoort, Donald (2006), "Internal Controls After Sarbanes-Oxley: Revisiting Corporate Law's Duty of Care as Responsibility for Systems", 31 J. Corp. L. 949, p.954

47 Jacobs, Edwin (2005), "Security as a Legal Obligation", disponible en: <http://www.arraydev.com/commerce/JIBC/2005-08/security.htm>, última visita: noviembre 29, 2009.
PWC (2006), "The Global State of Information Security", p.4

3. SEGURIDAD DE LA INFORMACIÓN DENTRO DE LA RACIONALIDAD CORPORATIVA

El objetivo de esta Sección es proveer argumentos para elevar la Seguridad de la Información como un tema de Gobierno Corporativo. Por lo tanto, en primera instancia, se argumentará que la Seguridad de la Información no se encuentra actualmente incluida en el Gobierno Corporativo y explica las razones para ello desde la perspectiva de tres funciones corporativas (la Junta Directiva, el Departamento Legal y el Departamento de Tecnología). Luego la sección expone los efectos del divorcio entre la Seguridad de la Información y el Gobierno Corporativo y describe el impacto negativo de que una endeble Seguridad de la Información en el cumplimiento de los objetivos del Gobierno Corporativo.

3.1 Seguridad de la información fuera del gobierno corporativo

Desde la perspectiva de la Junta Directiva, la habilidad limitada para medir el costo-beneficio y el retorno de la inversión de las medidas de seguridad representa un obstáculo para integrar la Seguridad de la Información en el Gobierno Corporativo. En otras palabras, la Seguridad de la Información continúa sufriendo del problema fundamental de no representar un caso de negocios , lo que se explica en parte porque la mayoría de los profesionales de los Departamentos de Tecnología cuentan con una formación técnica y no comercial. Adicionalmente, muchos de los beneficios son intangibles o difíciles de medir, tales como la reducción en las horas pérdidas del personal o la prevención del daño en la reputación de la compañía[49].

49 The Information Assurance Advisory Council (2002), op. cit., p. 8

En relación con la función Legal, el uso de la Teoría de la Agencia (*Agency Theory*) ha llevado a muchos abogados a entender el Gobierno Corporativo sólo como el marco normativo (reglas e instituciones) que determina el control y dirección de la compañía y que define las relaciones entre los participantes primarios de la sociedad (administradores y asociados). En términos generales, la Teoría de Agencia identifica la relación donde una parte, el principal, delega un trabajo en otra, el agente. Este divorcio de la propiedad y el control en una compañía crea un reto a los intereses de los accionistas, ya que el oportunismo o el egoísmo del agente puede llevarlo a actuar en contra de los mejores intereses del principal, lo cual ha sido confirmado por los bien conocidos escándalos de Enron y otras empresas[50].

Lo anterior tiene como resultado que el Gobierno Corporativo tiende a ser visto por los abogados básicamente en términos de legitimidad, responsabilidad y eficiencia de los poderes ejercidos por los administradores. Este es un problema porque la sostenibilidad y la sobrevivencia de una compañía no dependen exclusivamente del eventual abuso de los administradores, sino también de otros temas (e.g., de la Seguridad de la Información) que son finalmente relegados a un simple tema de cumplimiento normativo, el cual es precisamente el caso de la Seguridad de la Información debido al incremento en la normatividad sobre la materia. Por ejemplo, la Encuesta sobre Crimen y Seguridad Informática realizada en 2008 (*Computer Crime and Security Survey o Encuesta CSI*) encontró que el cumplimiento de las normas sobre protección de datos personales para las compañías es un tema muy sensible relacionado con la seguridad de los computadores[51].

Finalmente, análisis históricos demuestran que la mayoría de las organizaciones han atendido las preocupaciones de seguridad desde la perspectiva de varias funciones dentro de la organización, normalmente, de manera desintegrada. Esto es, en parte, debido a que la seguridad de la información ha sido vista, principalmente, como un tema tecnológico, y tal seguridad se ha ocupado de mantener alejados a los posibles delincuentes[52]. La función de tecnología tiende a usar diferente terminología, con poco en común con otras funciones corporativas[53]. Como consecuencia, el Departamento de Tecnología se está alejando de una aproximación estratégica para enfocarse exclusivamente en la respuesta técnica. Por ejemplo, de acuerdo con el Estado Global de la Seguridad de la Información de 2006 (*2006 Global State of Information Security*), los ejecutivos del Departamento de Tecnología están cambiando de unas practicas más estratégicas hacia otras más tecnológicas. En el año 2005, por cada elemento tecnológico en la lista de tareas de un ejecutivo de la seguridad, había cuatro procesos estratégicos; proporción que en el año 2006 era cercana 1 a 1. Adicionalmente, siete de los doce temas más importantes en la lista de tareas de seguridad son procesos de ajuste tecnológico, incluyendo creación de copias de seguridad, firewalls y la implementación de esquemas de identificación como contraseñas[54].

3.2 Implicaciones del divorcio entre la seguridad de la información y el gobierno corporativo

El hecho de que la Seguridad de la Información sea manejada por fuera de las directrices de la Junta Directiva y considerada como un simple problema técnico o un mero asunto de cumplimiento normativo tiene como resultado

50 Salacuse, Jeswald, *op. cit.*, p.71

51 CSI (2008), "CSI Computer Crime and Security Survey", *Computer Security Institute.*

52 Deloitte, op. cit., p. 17

53 IT Governance Institute, op. cit., p.14

54 PWC, op. cit., p.7.

una pobre solución al problema que genera consecuencias legales y económicas negativas para la compañía, y que compromete los objetivos del Gobierno Corporativo. Lo anterior es evidente en dos efectos particulares.

El primer efecto es que las respuestas tecnológicas pueden convertirse en métodos ineficientes para resolver el problema. Por ejemplo, los *firewalls* y el software de detección de intrusos son usualmente efectivos para detener hackers, pero si la mayor vulnerabilidad de la compañía son descuidados (o maliciosos) empleados que de manera inadvertida (o intencional) revelan contraseñas, incluso la más sofisticada medida técnica no resolverá el problema[55].

En segundo término, las compañías tienden a manejar la Seguridad de la Información como un cálculo de costos. La seguridad continúa siendo vista y calculada como un costo, no como algo que puede adicional valor estratégico y, en consecuencia, ser traducido en ingresos o ahorros importantes[56]. Las firmas están usualmente bajo presiones económicas para maximizar utilidades y sólo inician nuevas actividades cuando hacerlo es rentable. Con relación a la Seguridad de la Información, se puede esperar que las compañías inviertan en ella desde la perspectiva de una entidad que maximiza beneficios. En otras palabras, las firmas buscarán decidir sus gastos en seguridad de acuerdo con el nivel de la responsabilidad legal y los riesgos financieros que estén dispuestos a asumir en caso de presentarse un incidente de seguridad[57].

El problema subyacente de esta situación es que las compañías pueden fallar en asumir la totalidad de los costos de los incidentes de seguridad ya que muchas entidades no son declaradas como responsables por todos los costos causados. Primero, un incidente de seguridad en una compañía puede causar daños a otra, sin que tal situación sea rastreable o en relación con la cual no exista recurso legal disponible. La información sustraída, por lo general, carece de indicación alguna de su lugar de origen. Entonces, si la entidad afectada permanece en silencio, el público será incapaz de identificar el lugar de donde la información fue sustraída. Como consecuencia, los consumidores no podrán asociar el daño que ellos sufren con la empresa que permitió el incidente. Segundo, en temas relacionados con información financiera, la institución puede escapar de la responsabilidad frente a otra institución porque la ley normalmente asigna el riesgo financiero de ciertos incidentes de seguridad a la entidad que equivocadamente confió en la información fraudulentamente presentada (e.g., otorgar una nueva tarjeta de crédito, aprobar un crédito o acreditar una transferencia electrónica) en lugar de asignar el riesgo a la entidad que permitió que ocurriera el incidente.

3.2.1 Consecuencias económicas

Los incidentes relacionados con la Seguridad de la Información generan un impacto negativo en términos económicos, los cuales ponen en riesgo la sostenibilidad de las compañías. Esta afirmación es validada por cuatro métodos: el primero de ellos consiste en medir el daño causado por el incidente en sí. El segundo analiza la inversión realizada para evitar incidentes de seguridad. El siguiente toma en cuenta el daño que es causado en la reputación de la firma involucrada. El último método dirige su atención a la reducción del precio de la acción de la compañía atacada.

El primer método requiere examinar los diferentes tipos de incidentes de seguridad de manera separada, ya que considera que algunos problemas

55 Smedinghoff, Thomas (2007), "Director Responsibilities for Data Security: Key Questions the Board Should Ask", *IT Security, Directors Monthly*, p.20

56 PWC, op. cit.,p.4.

57 Schwartz, Paul and Janger, Edward, *op. cit.*, p.927

imponen altos costos preventivos y correctivos, mientras que otros problemas no son más que una simple distracción. Por ejemplo, mientras Blaster, un muy conocido *worm,* hizo un poco más que disminuir la velocidad de procesamiento de los computadores personales, el *Love Bug* reescribió y corrompió archivos, causando 10 billones de dólares en daños[58].

Una categoría de ataque es aquella que tiene la habilidad de dañar sistemas informáticos, tales como sacar de línea a una red o borrar datos. Restaurar una red o recrear la información perdida usualmente impone cuantiosos costos para la víctima de un ataque. De acuerdo con la encuesta CSI/FBI, en Estados Unidos la amenaza más costosa son los virus, representando 15.7 millones de dólares[59]. Por otra parte, en 2003 la FTC identificó al rededor de 48 billones de dólares en pérdidas de instituciones y 5 billones adicionales de pérdidas sufridas por individuos[60]. Adicionalmente, la Encuesta de Deloitte de 2006 (*2006 Deloitte Survey*), afirma que el 72 por ciento de las instituciones financieras afectadas sufrió un daño, incluyendo costos directos e indirectos, en el rango de un millón de dólares, mientras que el 2 por ciento de ellos siente que el número es superior a los 5 millones de dólares[61].

El otro efecto de un ataque es causar daño a las operaciones de negocio, incluyendo pérdida en ventas, mientras que un sitio de comercio electrónico es deshabilitado por cualquier medio (en especial por DoS). Ahora bien, a pesar de que una compañía puede percibir una pérdida general en las ventas, estimar la suma del daño es mucho más especulativo que determinar los costos laborales tangibles de activar la red nuevamente. Considérese una librería virtual que es deshabilitada por un ataque pero que vuelve a funcionar en una hora. ¿Qué porción de las ventas esperadas se perdió? Los consumidores habrían podido comprar sus libros de otra página que estuviera disponible o ellos pudieron haber comprado los libros en su librería local en lugar de usar Internet. En ambos casos significa que el vendedor afectado sufrió una pérdida de todas las ventas esperadas en el periodo que la página estuvo deshabilitada. Alternativamente, los consumidores pudieron simplemente haber esperado hasta que su proveedor de libros en línea estuviera de vuelta, caso en el cual no se presenta ninguna pérdida[62].

El último tipo de consecuencia que un ataque es capaz de causar es la disminución de la confianza de los clientes y usuarios con relación a su información personal. Por ejemplo, en el Reino Unido una encuesta realizada por la Oficina del Comisionado de la Informaciòn (*Information Commissioner's Office*) demostró que alrededor del 84 por ciento de la gente desconfía en la forma en que las páginas de Internet manejan su información personal[63], el cual, si bien es muy difícil de cuantificar, puede llegar a ser sustancial[64].

El segundo método para evaluar el impacto económico de las amenazas a la seguridad de los sistemas de información analiza qué tanto esfuerzo hace el usuario para evitar los incidentes de seguridad. La cantidad de dinero que una firma está dispuesta a gastar para evitar el problema puede ser interpretado como el límite más bajo del daño esperado que el problema puede causar. Por ejemplo, de acuerdo con la Encuesta CSI/FBI, el 47 por ciento de las organizaciones

58 Hahn, Robert and Layne-Farrar, Anne (2006), "The Law and Economics of Software Security", 30 Harv.J.L.& Pub. Pol'y 283, p.308

59 CSI/FBI (2006), "Computer Crime and Security Survey", Computer Security Institute, p.13.

60 Ibid. p.22

61 Deloitte, op. cit., p.28

62 Hahn, Robert and Layne-Farrar, Anne, op. cit., p. 307

63 LexisNexis News Analysis, "Survey reveals internet security concerns", disponible en: <http://lexisnexis.butterworths.co.uk/law/index.htm?bAuth=no> , última visita: noviembre 29, 2009.

64 Hahn, Robert and Layne-Farrar, Anne, op. cit., p. 303

asignan alrededor del 3 por ciento del total de su presupuesto de tecnología y el 34 por ciento de ellas más del 5 por ciento. Esto representa una cifra considerable que ha aumentado dramáticamente en los últimos años, particularmente, para las medianas y pequeñas compañías[65]. En relación con las instituciones financieras, el nivel de gasto en la Seguridad de la Información también está en alza. El 95 por ciento de los participantes de la Encuesta de Deloitte de 2006 indicó que ha experimentado alguna forma de crecimiento en los presupuestos de Seguridad de la Información, aumento que llegó a ser del 10 por ciento para más del 20 por ciento de los participantes[66].

El tercer método se relaciona con la lesión a la reputación que una empresa sufre como consecuencia de los incidentes de seguridad. La revelación de los incidentes de seguridad tiene el efecto de avergonzar a las compañías resaltando la ausencia de mecanismos adecuados de seguridad. Los individuos, negocios y otras organizaciones pueden ser afectados profundamente por la circulación de noticias sobre su comportamiento anterior. Por consiguiente, las personas que adoptan las decisiones se preocupan de la reputación de sus empresas y buscan tanto evitar las sanciones sociales contra ellos, como ganar la aprobación social. También los negocios pueden temer la pérdida de clientes y otras oportunidades si un incidente se hace público y la reputación de la institución responsable se ve afectada[67]. Por ejemplo, la encuesta de CSI/FBI establece que la razón predominante dada por no informar los incidentes de seguridad es la percepción que la publicidad negativa puede dañar la imagen de sus organizaciones[68].

El último método se refiere al impacto negativo que un incidente de seguridad puede causar en la valoración de la acción de una sociedad listada en bolsa. Un estudio empírico encontró evidencia de la reacción negativa del mercado accionario frente a los anuncios de incidentes de seguridad publicados en los periódicos. En particular, el estudio encontró que no todos los tipos de incidentes generan los mismos impactos económicos. Por una parte, no hay una reacción significativa del mercado cuando el incidente no está relacionado con la confidencialidad (ataques tales como DoS, virus y worms). En contraste, sí hay una reacción significativa para aquellos incidentes que se relacionan con violaciones a la confidencialidad, por ejemplo, el acceso no autorizado a información sobre tarjetas de crédito o la publicación indebida de información confidencial[69]. A pesar de que este estudio tiene una limitación importante, ya que la muestra probablemente no es representativa del número total de incidentes de seguridad[70], las conclusiones del estudio han sido validadas en la práctica. Por ejemplo, ChoicePoint experimentó más del 20 por ciento de disminución en el valor de su acción luego de sufrir un muy serio incidente de seguridad[71].

3.2.2 Consecuencias legales

Las consecuencias legales de un incidente de seguridad son el efecto natural del incumplimiento a la obligación legal de proveer seguridad, y pueden ser clasificadas en tres tipos. Primero, la imposición de sanciones por la falta de cumplimiento de una regulación que persigue objetivos diferentes a la Seguridad de la Información. Esta consecuencia se deriva directamente de la legislación en si. Por

65 **CSI/FBI, op. cit., p6.**

66 **Deloitte, op. cit., p.24**

67 **Schwartz, Paul and Janger, Edward, op. cit., p.929-931**

68 **CSI/FBI, op. cit., p6.**

69 Campbell, Katherine, et. al. (2003), "The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence From The Stock Market", Journal of Computer Security 11 431–448, p.445

70 Ibid, p. 446

71 Smedinghoff, Thomas (2006), "The Challenge of Electronic Data: Corporate Legal Obligations to Provide Information Security", Wall Street Lawyer, Vol. 10 No. 3, p.6

ejemplo, el incumplimiento de los requerimientos de SOX puede resultar en sanciones penales de hasta 1 millón de dólares y de 10 años de prisión por violaciones culposas, y hasta de 5 millones de dólares y 20 años de prisión por violaciones dolosas[72].

El segundo tipo de consecuencias legales son los litigios civiles que las victimas de los incidentes de seguridad pueden iniciar, en particular, en casos de suplantación de identidad. Sin embargo, los casos que se han generado por incidentes de seguridad ampliamente conocidos, a pesar de usar varias teorías legales[73], han mostrado que los demandantes enfrentan obstáculos cuando tratan de demostrar la responsabilidad de las empresas cuyos sistemas son vulnerables. Esto sugiere que la violación de la privacidad por si sola no es fundamento suficiente para que demandas por responsabilidad sean exitosas en contra de los administradores de información personal. En términos generales, los demandantes han fallado en dos frentes. En primer lugar, no han logrado establecer un daño real, concreto y particularizado[74]. Por ejemplo, en *Bell vs. Acxiom*[75], una acción de clase en los Estados Unidos, la demandante alegó que su privacidad había sido puesta en peligro y que existía un mayor riesgo de que su identidad fuera suplantada como resultado del acceso no autorizado a los computadores de Acxiom. Sin embargo, la demandante falló en probar que su información había sido realmente incluida en la información sustraída. En consecuencia, su pretensión de daño fue limitada a un incremento en el riesgo de suplantación de identidad que no fue considerado por la corte como un daño concreto, ya que éste simplemente se refería a un potencial daño futuro. La segunda falencia de los demandantes es que no han mostrado un vínculo causal entre las acciones de los demandados y el perjuicio causado. Entonces, así el demandante pudiera mostrar que sido víctima de un robo de identidad, es difícil establecer que ese perjuicio fuera razonablemente producto del incidente de seguridad ocurrido en los sistemas del demandado. Por ejemplo, en *Stollenwerk vs. Tri-West*[76], el hecho de que la información del demandante fuera usada para abrir cuentas fraudulentas no fue suficiente para establecer el vínculo de causalidad porque el demandante pudo haber revelado la misma información a otras partes. Como un obstáculo adicional, las acciones de clase sobre privacidad o seguridad de la información pueden estar bloqueadas en caso de que los usuarios hayan acordado arbitramento obligatorio para la solución de disputas[77]. En *Cunningham vs. Citigroup*[78] un acuerdo suscrito por los demandantes cuando ellos abrieron cuentas bancarias limitó a los consumidores a acudir a arbitramentos para todo reclamo en contra del banco, aislando al demandado del escrutinio de una corte federal[79].

La otra consecuencia legal son las sanciones administrativas provenientes de las agencias gubernamentales por temas relacionados con Seguridad de la Información. Los resultados de las investigaciones administrativas (incluso relacionadas a los mismos casos considerados por las Cortes) indican que los incidentes de seguridad conllevan serias consecuencias legales, incluyendo elevadas multas.

72 Sections 302 and 304

73 Por ejemplo, incumplimiento de contrato, incumplimiento de obligaciones fiduciarias y negligencia.

74 Kennedy, John and Sanjanwala, Parishi (2007), "Civil Suits Arising from Information Security Breaches", Volume 237, 2/2/2007 N.Y.L.J. 4, (col. 4).

75 Bell v. Acxiom Corp., No. 4:06CV0045-WRW, 2006 WL 2850042, slip. op. (E.D. Ark. Oct. 3, 2006).

76 Stollenwerk v. Tri-West Healthcare Alliance, 2005 WL 2465906 (D. Ariz. Sept. 6, 2005)

77 Wolf, Christopher (2006), "Consolidated Case Dismissed When Arbitration Clauses Presented", *183 N.J.L.J. 1166, No. 13.*

78 No. 05-3476, 2005 U.S. Dist. LEXIS 33805 (D.N.J. Dec.16, 2005)

79 Wolf, Christopher, op. cit.

En los Estados Unidos, la FTC ha compelido a las empresas a proveer Seguridad de la Información mediante el uso de dos aproximaciones: (i) teorías contractuales; y (ii) considerando como desleales las prácticas de negocio inseguras. Usando la teoría contractual, la FTC tomó la posición de que el incumplimiento de las promesas hechas con relación a la protección de la información confidencial de los clientes permite (bajo la Ley de la FTC o *FTC Act*) prohibir actos engañosos o desleales o prácticas que afecten el mercado[80]. Por ejemplo, en Petco[81] la FTC argumentó que Petco tuvo fallas en la seguridad de su página web que violaban su política de privacidad en línea y que, contrario a los argumentos de Petco, dicha compañía no había tomado los pasos razonables o apropiados para prevenir ataques[82]. Otro notorio incidente que fue resuelto usando la teoría contractual involucró a ChoicePoint. Este caso es significativo por la multa impuesta por la FTC, ya que el investigado fue relevado de los cargos a cambio del pago de 10 millones de dólares en sanciones civiles y un monto adicional de 5 millones de dólares para reparaciones a los clientes[83]. Usando la segunda aproximación citada, la FTC ha iniciado acciones cuando consideraba que las prácticas de seguridad de las compañías eran desleales. El primer caso fue BJ´s *Wholesale Club*[84], donde la FTC argumento que BJ´s inició una serie de prácticas que, tomadas en conjunto, no proveían seguridad razonable. La FTC alegó que la falla de BJ´s de asegurar la información sensible de sus clientes constituía una práctica desleal porque causó un perjuicio sustancial que no podía ser evitado por los consumidores[85].

80 Matus, Wayne (2006), "Security Breaches. Are You Prepared for Litigation and a Consent Order?", *866 PLI/Pat 117*, p.124

81 FTC File No. 032-3221, Docket No. C-4133 (Nov. 17, 2004)

82 Otros casos iniciales donde se alego que las compañías habían actuado de manera engañosa hacienda procesas expresas o implícitas sobre la protección de información sensible, que luego fueron incumplidas involucran a Eli Lilly & Co., Microsoft, Guess, Inc., and Tower Records. Matus, Wayne, *op. cit.*, p.127

83 *ibid*, p.130

84 BJ's Wholesale Club, Inc., File No. 042 3160 (FTC consent order approved Sept. 2005).

85 Ballon, Ian (2007), op. cit., p.215.

4. SEGURIDAD DE LA INFORMACIÓN COMO UN TEMA DE GOBIERNO CORPORATIVO

Esta sección expone las razones de integrar Seguridad de la Información y Gobierno Corporativo. Así mismo, la Sección argumenta que la aplicación de los principios de Relevación y de Manejo de Riesgo es un método efectivo para lograr dicha integración.

4.1 ¿Por qué la seguridad de la información debe ser un tema de gobierno corporativo?

Con miras a proteger la supervivencia de los negocios, las organizaciones deben, continuamente, ajustar y alinear sus estrategias, sus operaciones, su estructura de gobierno y la forma que se toman decisiones, lo cual les permite ser proactivos en identificar, y rápidamente ajustarse a los riesgos[86]. La Seguridad de la Información debe ser un proceso que inicie en la cima de la pirámide empresarial y se extienda hacia la base, enlazando los procesos estratégicos del negocio y siendo aplicable a todas las funciones de la organización[87]. Si la Seguridad de la Información es manejada como un tema de Gobierno Corporativo, el problema podría ser resuelto de una mejor manera porque la compañía podría integrar varios componentes de la organización (negocio, gobierno, tecnologías de la información, Seguridad de la Información y función legal)[88]. En el mismo sentido, la Norma ISO 27001:2005, que es un estándar creado por la Organización

86 Deloitte, op. cit., p.15, and Ernst & Young (2006), "Global Information Security Survey", p.10

87 IT Governance Institute, op. cit., p.16

88 Ernst & Young, op. cit., p.10

Internacional de Estándares y aceptado internacionalmente para la administración de la Seguridad de la Información de todo tipo de organizaciones, sugiere que la adopción de un sistema de administración de la Seguridad de la Información debe ser una decisión estratégica de la organización, pues depende de las necesidades, objetivos, requerimientos específicos de seguridad, procesos, tamaño y la estructura particulares de la empresa[89]. Este enfoque podría crear un marco coherente para la toma de decisiones, principios y responsabilidades, identificando los procesos y el personal para el monitoreo y cumplimiento de los objetivos, y crear una cultura de buen gobierno, en lugar de una cultura enfocada a las acciones reactivas o de auditoría. Por ejemplo, la Encuesta Global del Estado de la Seguridad de la Información (*Global State of Information Security 2006*) considera aquellas organizaciones que integran y alinean la seguridad con las estrategias y procesos de negocio son capaces de reducir el número de ataques exitosos y la resultante pérdida financiera[90].

No obstante, evitar los impactos negativos no es el único beneficio de tener una sólida Seguridad de la Información. Una buena seguridad puede mejorar la reputación, activar estrategias en línea, incrementar la confianza de otros con quien se hacen negocios, e incluso puede mejorar la eficiencia reduciendo el tiempo y el esfuerzo desperdiciado en recuperarse luego de un incidente de seguridad[91]. En particular existen dos beneficios concretos. Primero, con buena planeación y las medidas de seguridad apropiadas, las organizaciones pueden tomar ventaja de la importancia en la protección de los datos, la significancia del debate sobre privacidad y la preocupación pública relacionada con el 'cyber-crimen' para incrementar sus negocios, ganar la confianza de los clientes y potencialmente obtener una ventaja competitiva en el mercado. La Seguridad de la Información es una extensión de la política de servicio al cliente, la cual construye una marca más reconocida y una mejor lealtad de los clientes, puesto que genera relaciones de confianza[92]. Esto también es detectado por la Norma ISO 27001 que señala que el aumento en la confianza de los clientes y socios estratégicos por la garantía de calidad y confidencialidad comercial es un beneficio directo de la implementación de un sistema de manejo de la Seguridad de la Información[93]. Segundo, la Seguridad de la Información ha tenido su propio aspecto social por la protección a los datos personales, a la privacidad y al concepto de ser un buen ciudadano, ya que la Seguridad de la Información puede ser fácilmente comprometida por las débiles prácticas de otra persona. Entonces, debe ser una prioridad de cada compañía el evitar convertirse en un punto vulnerable a los ataques, lo cual debe ser extendido a sus proveedores y consumidores. En adición, en la medida en que la Responsabilidad Social Empresarial gana relevancia en el mercado, las medidas que promueven un uso ético de las nuevas tecnologías en la Seguridad de la Información se hacen más importantes[94].

4.2 Principios de gobierno corporativo aplicados a la seguridad de la información

La Junta Directiva y la alta gerencia cuenta con una serie de herramientas disponibles para implementar las estrategias de gobierno en la gestión de la Seguridad de la Información. Por

89 Corletti, Alejandro (2006), "Manual de Análisis de ISO-27001:2005", desarrolloweb.com, disponible en <http://www.desarrolloweb.com/manuales/77/>, última visita: junio 16, 2010.

90 PWC, op. cit., p.4

91 IT Governance Institute, op. cit., p.14

92 The Information Assurance Advisory Council, *op. cit.*, p.29

93 Ver: www.iso27001.es

94 *Ibid.*, p.30

ejemplo, los directivos pueden identificar los activos informáticos; adelantar análisis periódicos de riesgos, diseñar, implementar y actualizar un plan de seguridad formal que efectivamente se encargue de las amenazas que la organización enfrenta; proveer entrenamiento a los empleados; y diseñar planes de continuidad en caso de que se presente un incidente de seguridad[95]. Dentro de tales herramientas, la presente sección mostrará cómo los principios de Relevación y de Manejo de Riesgo del Gobierno Corporativo constituyen herramientas útiles para integrar Seguridad de la Información y Gobierno Corporativo.

4.2.1 Revelación

El estado de la Seguridad de la Información en las compañías y los incidentes de seguridad ocurridos deben ser comunicados a los interesados con el objeto de cumplir con el principio de Gobierno Corporativo de revelar los aspectos críticos de las compañías. Este mandato es también soportado por provisiones legales las cuales requieren tal revelación en ciertas circunstancias.

La Revelación es usualmente justificada como una forma de proveer a los inversionistas en el mercado secundario una protección comparable a aquella con la que cuentan los inversionistas del mercado primario[96]. Sin embargo, el principal beneficio social de la Revelación es su influencia en el Gobierno Corporativo porque contribuye al ejercicio de los derechos de los accionistas, al monitoreo de las corporaciones y al desarrollo de una disciplina en la administración[97]. La Revelación mejora el Gobierno Corporativo ayudando a los accionistas a hacer cumplir las obligaciones de los administradores e incrementa el desempeño de los administradores. Sin esquemas de revelación, los administradores están inclinados a no proveer información que pueda sugerir la existencia de una violación de una de sus obligaciones o deberes, haciendo casi imposible que los accionistas conozcan la eventual violación[98]. En adición, cuando los administradores tienen la obligación legal de revelar cierta información, se ven avocados a investigar y analizar información que de otra forma podrían ignorar, por ejemplo, cierto tipo de información negativa. La Revelación, debido a su énfasis en información negativa, puede ayudar a corregir el problema en operaciones existentes que de otra forma no serían reportadas[99].

Ahora bien, los temas relacionados con la Seguridad de la Información deben ser revelados debido a su importancia y a su naturaleza riesgosa. Por ejemplo, los Principios de la OECD establecen que: "El marco para el gobierno corporativo deberá garantizar la divulgación oportuna y precisa de todas las cuestiones materiales relativas a la sociedad (...). Un régimen divulgativo fuerte, que promueva una transparencia real, es una característica fundamental en el ámbito de la monitorización de sociedades basada en el mercado, y esencial para la capacidad de los accionistas para ejercitar sus derechos de propiedad de forma documentada"[100].

Por otro lado, la legislación también impone la obligación de relevación del estado de la seguridad corporativa y de los incidentes de seguridad ocurridos.

95 Smedinghoff, Thomas (2007), op. cit.. Otros artículos que comentan las herramientas con las que cuenta la Junta Directiva en relacion con la Seguridad de la Información in son: Baye, Larry (2007), "Strategies for Implementing Information Security Systems", 894 PLI/Pat 243 and Benjamin, Barry (2006), "Information Security. More Than Just Consumer Notification, and Already Here", 9/06 Metro. Corp. Couns. 21, (col. 1).

96 Fox, Merritt (1999), "Required Disclosure and Corporate Governance", 62-SUM Law & Contemp. Probs. 113, p.115.

97 Salacuse, Jeswald, op. cit., p.73

98 Fox, Merritt, op. cit., p.118.

99 Ibid. p.123-125

100 OECD Principles, p.49

En relación con el estado de la Seguridad de la Información, se ha sugerido en los Estados Unidos que los requerimientos de la sección 303 de la regulación de la Security and Exchange Commission (SEC) deben ser interpretados de tal forma que incluyan las capacidades de seguridad de la información corporativa[101]. La citada sección requiere a las compañías revelar tendencias e incertidumbres que afectan la liquidez y los recursos de capital, por ende es posible argumentar que los temas de Seguridad de la Información deben ser revelados. De acuerdo con la SEC, "para identificar tendencias, demandas, compromisos, eventualidades e incertidumbres que requieran revelación, la administración debe considerar (...) circunstancias que puedan perjudicar la habilidad del emisor para continuar con la suscripción de transacciones que ha sido integral a las operaciones históricas o son financiera y operacionalmente esenciales"[102].

Tratándose del tema de los incidentes de seguridad, la legislación norteamericana ha creado la obligación de revelación de los incidentes que afectan la información personal, generando dos efectos. Por una parte, la ley impone una sanción a la reputación de las empresas porque la institución que sufre el ataque es obligada a revelar su identidad al consumidor cuya información fue comprometida y a reconocer que fue el origen del incidente. En consecuencia, la relevación motiva a las empresas a invertir en la seguridad de los datos personales para evitar la notificación y el consecuente daño en su reputación[103]. Por otra parte, la notificación de los incidentes también cumple la función de mitigar el daño porque supone que permite a los consumidores y a otros procesadores de información personal protegerse de daños adicionales que pueden causarse por el incidente ocurrido[104].

4.2.2 Manejo del riesgo

Las organizaciones tienen que mejorar su sistema de manejo del riesgo para cumplir con sus estrategias de negocio y para tomar ventajas de las oportunidades sin poner el futuro de la compañía en un peligro innecesario. Los Principios OECD explican el principio de Manejo del Riesgo de la siguiente manera: "El Consejo deberá desempeñar determinadas funciones clave, que incluyen: 1. La revisión y orientación (...) de la política de riesgos"[105] y reconoce que "un ámbito de creciente importancia para los Consejos, y que guarda una relación estrecha con la estrategia de la empresa, es la política de riesgos. Esta política abarcará la especificación de los tipos y grados de riesgo que una sociedad está dispuesta a aceptar en su intento por cumplir sus objetivos. Constituye, por tanto, una directriz vital para los directivos encargados de gestionar riesgos para alcanzar el perfil de riesgo deseado por la sociedad"[106]. Finalmente, el mismo documento argumenta que las Juntas Directivas tienen que "garantizar la integridad de los sistemas de gestión del riesgo"[107].

En el Reino Unido temas de Gobierno Corporativo y Manejo del Riesgo también se han desarrollado de manera conjunta. Las recomendaciones del Comité Hampel sobre Gobierno Corporativo[108] amplió el concepto de control interno para atender, entre otros aspectos, análisis de riesgo

101 Matwyshyn, Andrea (2005), "Material Vulnerabilities: Data Privacy, Corporate Information Security and Securities Regulation", Berkeley Electronic Press, disponible en <http://law.bepress.com/expresso/eps/524>, última visita: noviembre 29, 2009.

102 SEC Release No. 33-8056 (Jan. 22, 2002), disponible en <www.sec.gov/rules/other/33-8056.htm>, última visita: noviembre 29, 2009.

103 See: Section 4.2.1

104 Schwartz, Paul and Janger, Edward, op. cit., p.936-937

105 OECD Principles, p.60

106 Ibid., p.60

107 Ibid., p.62

108 Hampel, Ronald (1998), "Final Report. Committee on Corporate Governance".

y su respuesta[109]. Hampel tomó una perspectiva amplia del control interno, argumentando que los administradores deben establecer un sistema robusto de manejo del riesgo para identificar y evaluar riesgos potenciales en la operación de la empresa[110]. Menos de dos años después, el Reporte Turnbull fue lanzado y tomó la existencia de un riguroso sistema de manejo del riesgo como indicativo de un efectivo control interno[111]. El énfasis del Reporte Turnbull en el control del riesgo es que el manejo del riesgo y control debe ser embebido por los procesos de negocio[112].

Por su parte, la gestión del riesgo es una elemento esencial de la Norma ISO 27001:2005, puesto que no se puede gestionar el riesgo si éste no ha sido medido. Las organizaciones que pretenden seguir las recomendaciones de dicha norma u obtener una certificación basada en la misma requieren medir y evaluar los riesgos de seguridad que enfrentan así como revisar y reevaluar los riesgos en una etapa futura para asegurar que se tiene implantado una eficaz Seguridad de la Información. La Norma ISO 27001:2005 propone un proceso que ayuda a la organización a evaluar el riesgo y que contempla las siguientes fases: (i) Identificación y tasación de activos; (ii) Identificación de los requerimientos de seguridad; (iii) Evaluación de la posibilidad que las amenazas y vulnerabilidades ocurran; (iv) Cálculo de los riesgos de seguridad; (v) Selección de opciones de tratamiento de los riesgos; y (vi) Selección de controles para reducir el riesgo a niveles aceptables[113].

Los líderes de las compañías están empezando a reconocer que la Seguridad de la Información necesita tener un permanente espacio en las discusiones sobre Manejo del Riesgo para identificar y administrar, de manera proactiva, otras áreas de riesgo empresarial y reducir los incidentes. Cerca de dos tercios de los participantes de la Encuesta Global de la Seguridad de la Información realizada por Ernst & Young en 2006 dijeron que sus compañías usan reuniones periódicas y marcos formales para asegurar el envolvimiento en la Seguridad de la Información. Un creciente porcentaje de los participantes en la encuesta (43 por ciento comparado con el 40 por ciento en 2005) dijo que la Seguridad de la Información esta integrada con sus programas y procesos de manejo del riesgo[114]. Sin embargo, más de la mitad de los participantes aún necesitan tomar pasos para integrar el manejo del riesgo informático dentro de sus actividades generales de manejo del riesgo[115].

109 *Ibid.*, p.53–54

110 Drennan, Lynn and Beck, Matthias (2001), *"Corporate Governance: A Mandate for Risk Management?"*, Caledonian Business School, Glasgow Caledonian University, disponible en: <www.nottingham.ac.uk/business/cris/ukec/2001paper4.doc>, última visita: noviembre 29, 2009.

111 Institute of Chartered Accountants in England & Wales (1999), *Internal Control: Guidance for Directors on the Combined Code, Accountancy Books.*

112 Drennan, Lynn and Beck, Matthias, *op. cit.*

113 Alexander, Alberto (2008), *"Análisis del Riesgo y el Sistema de Gestión de Seguridad de la Información: El Enfoque ISO 27001:2005", Eficiencia Gerencial y Productividad"*, disponible en: <http://www.iso27000.es/download/Analisis_del_Riesgo_y_el_ISO_27001_2005.pdf>, última visita: junio 16, 2010.

114 Ernst & Young, op. cit., p.12

115 Ibid., p.10

CONCLUSIONES

Por una parte, el objetivo de un sólido Gobierno Corporativo es la base para un éxito organizacional a largo plazo o, en términos de los Principios OECD, "un elemento clave para aumentar la eficacia económica y potenciar el crecimiento, así como para fomentar la confianza de los inversores"[116]. Por otra parte, la Seguridad de la Información es el proceso que pretende el aseguramiento de la confidencialidad, integridad y disponibilidad de la información, que están siendo seriamente amenazadas en la economía interconectada.

A pesar de la relevancia económica y legal de la Seguridad de la Información, ésta no se encuentra actualmente incluida en el Gobierno Corporativo. Esto lleva a las compañías a manejar de manera inarticulada la Seguridad de la Información como un costo, dando resultados pobres en la solución de los problemas y causando efectos negativos para la compañía. Contrariamente, si la Seguridad de la Información es elevada a un tema de Gobierno Corporativo, las funciones de la compañía podrían estar alineadas y el problema sería mejor atendido. Este método de resolver el problema no sólo ayuda a evitar los impactos negativos, sino que también mejora la reputación, activa estrategias en línea, incrementa la confianza de los socios de negocios e incluso aumenta la eficiencia.

Finalmente, para lograr la integración entre Seguridad de la Información y Gobierno Corporativo, los principios de Relevación y de Manejo del Riesgo son plenamente aplicables debido a la inherente naturaleza riesgosa de la Seguridad de la Información y a la creciente preocupación del público sobre este tema.

116 OECD Principles, p.11.

BIBLIOGRAFÍA

ALEXANDER, Alberto (2008), "Análisis del Riesgo y el Sistema de Gestión de Seguridad de la Información: El Enfoque ISO 27001:2005", Eficiencia Gerencial y Productividad", disponible en:<http://www.iso27000.es/download/Analisis_del_Riesgo_y_el_ISO_27001_2005.pdf>.

ATROSTIC, B.K. and SANG, Nguyen (2006), "How Businesses Use Information Technology: Insights for Measuring Technology and Productivity", CES 06-15, 2006

BAKER, Catherine (2000), "New Data Protection Act", Ent. L.R. 2000, 11(8), 193-196

BALLON, Ian (2007), "Internet Security Law and Litigation 2007: An Overview of FTC Enforcement Actions and Class Action Litigation", 903 PLI/Pat 207

BAYE, Larry (2007), "Strategies for Implementing Information Security Systems", 894 PLI/Pat 243
Bell v. Acxiom Corp., No. 4:06CV0045-WRW, 2006 WL 2850042, slip. op. (E.D. Ark. Oct. 3, 2006).

BENJAMIN, Barry (2006), "Information Security. More Than Just Consumer Notification, and Already Here", 9/06 Metro. Corp. Couns. 21, (col. 1).

BJ's Wholesale Club, Inc., File No. 042 3160 (FTC consent order approved Sept. 2005).

Cadbury Committee (Committee on the Financial Aspects of Corporate Governance) (1992), "The Report of the Committee on the Financial Aspects of Corporate Governance", London.

CAMPBELL, Katherine, et. al. (2003), "The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from The Stock Market", Journal of Computer Security 11 431–448

CERT Coordination Center (Octubre 2001), "Trends in Denial of Service Attack Technology", disponible en: <www.cert.org/archive/pdf/DoS_trends.pdf>.

CLAESSENS, Stijn (2006), "Corporate Governance and Development", Oxford University Press

COLBATH, Bruce (2006), "Customer Privacy and Data Security: The Importance of Guarding Your Henhouse", 60 Consumer Fin. L.Q. Rep. 603

CORLETTI, Alejandro (2006), "Manual de Análisis de ISO-27001:2005", desarrolloweb.com, disponible en <http://www.desarrolloweb.com/manuales/77/>.

Council Directive No. 95/46/EC of 24 October 1995 on the Protection of Individuals with Regard to the Processing of personal data and on the Free Movement of Such Data, O.J. L 281/31 (1995).
Council Directive No. 95/46/EC

CSI (2008), "CSI Computer Crime and Security Survey", Computer Security Institute.

CSI/FBI (2006), "Computer Crime and Security Survey", Computer Security Institute.

Data Protection Act 1998.
Deloitte (2006), "Global Security Survey 2006"

DRENNAN, Lynn and Beck, Matthias (2001), "Corporate Governance: A Mandate for Risk Management?", Caledonian Business School, Glasgow Caledonian University, disponible en: <www.nottingham.ac.uk/business/cris/ukec/2001paper4.doc>.

DTI (2006), "Information Security Breaches Survey", Technical Report.

Ernst & Young (2006), "Global Information Security Survey"

FOX, Merritt (1999), "Required Disclosure and Corporate Governance", 62-SUM Law & Contemp. Probs. 113

FTC File No. 032-3221, Docket No. C-4133 (Nov. 17, 2004)

HAHN, Robert and LAYNE-FARRAR, Anne (2006), "The Law and Economics of Software Security", 30 Harv.J.L.& Pub. Pol'y 283

HAMPEL, Ronald (1998), "Final Report. Committee on Corporate Governance".

HANNIGAN, Brenda (2003), "Company Law", LexisNexis

HARSHBARGER, Scott and JOIS, Goutam (2007), "Looking Back and Looking Forward: Sarbanes-Oxley and The Future of Corporate Governance", 40 Akron L. Rev. 1

Hewlett-Packard (2006), "Sarbanes-Oxley and the IT organization: A Survival Guide"

Institute of Chartered Accountants in England & Wales (1999), Internal Control: Guidance for Directors on the Combined Code, Accountancy Books.

IT Governance Institute (2006), Information Security Governance, Guidance of Boards of Directors and Executive Management, Second Edition

JACOBS, Edwin (2005), "Security as a Legal Obligation", disponible en: <http://www.arraydev.com/commerce/JIBC/2005-08/security.htm>.

KENDRICK, Rupert (2002), "Cyber-risks—How are You Managing Them?", 152 NLJ 7053.

KENNEDY, John and SANJANWALA, Parishi (2007), "Civil Suits Arising from Information Security Breaches", Volume 237, 2/2/2007 N.Y.L.J. 4, (col. 4).

KLOSEK, Jacqueline (2005), "Corporate Legal Departments, Third Edition", Practising Law Institute, Appendix A16. Privacy and Data Protection Law.

KOOPS (1999), The Crypto Controversy, A Key Conflict in the Information Society, Kluwer Law International.

LANGEVOORT, Donald (2006), "Internal Controls After Sarbanes-Oxley: Revisiting Corporate Law's Duty of Care as Responsibility for Systems", 31 J. Corp. L. 949

LexisNexis News Analysis, "Survey reveals internet security concerns", disponible en: <http://lexisnexis.butterworths.co.uk/law/index.htm?bAuth=no>.

MALLIN, Chistine (2007), Corporate Governance, Second Edition, Oxford

Marketplace Report: Monster.com Security Breach, disponible en: <http://www.npr.org/templates/story/story.php?storyId=13926368>.

MATUS, Wayne (2006), "Security Breaches. Are You Prepared for Litigation and a Consent Order?", 866 PLI/Pat 117

MATWYSHYN, Andrea (2005), "Material Vulnerabilities: Data Privacy, Corporate Information Security and Securities Regulation", Berkeley Electronic Press, disponible en: <http://law.bepress.com/expresso/eps/524>.

National Strategy to Secure Cyberspace, Febrero 14, 2003, disponible en: <www.whitehouse.gov/pcipb>.

OECD (2004), "Principles of Corporate Governance"

OECD (2004), "The OECD Principles of Corporate Governance. Policy Brief"

Public Company Accounting Reform and Investor Protection (Sarbanes-Oxley) Act of 2002, Pub. L. No. 107-204, 116 Stat. 745

PURSER, Steven (2004), A Practical Guide to Managing Information Security, Artech House
PWC (2006), "The Global State of Information Security"

R v. Lennon, Judgment of District Judge Kenneth Grant, Youth Court in Wimbledon, November, 2005.

REED, Chris and Angel, John (2007), Computer Law, Oxford, Sixth Edition

Reuters, "Monster.com Took 5 Days to Disclose Data Theft", disponible en: <http://investing.reuters.co.uk/news/articleinvesting.aspx?type=tnBusinessNews&storyID=2007-08-24T052725Z_01_WNAS2783_RTRIDST_0_BUSINESS-MONSTERWORLDWIDE-THEFT-DC.XML&pageNumber=1&imageid=&cap=&sz=13&tWModLoc=InvArt-C1-ArticlePage1>.

SALACUSE, Jeswald (2004), "Corporate Governance in the New Century", Comp. Law. 2004, 25(3)

SCHWARTZ, Paul and Janger, Edward (2007), "Notification of Data Security Breaches", 105 Mich. L. Rev. 913

SEC Release No. 33-8056 (Enero 22, 2002), disponible en: <www.sec.gov/rules/other/33-8056.htm>.

SHLEIFER, Andrei, and Vishny, Robert (1997), "A Survey of Corporate Governance", Journal of Finance, 52(2):737–83

SIEGEL, Kenneth (2007), "Protecting The Most Valuable Corporate Asset: Electronic Data, Identity Theft, Personal Information, and The Role of Data Security in The Information Age", 111 Penn St. L. Rev. 779

SMEDINGHOFF, Thomas (2006), "The Challenge of Electronic Data: Corporate Legal Obligations to Provide Information Security", Wall Street Lawyer, Vol. 10 No. 3

SMEDINGHOFF, Thomas (2007), "Director Responsibilities for Data Security: Key Questions the Board Should Ask", IT Security, Directors Monthly

Stollenwerk v. Tri-West Healthcare Alliance, 2005 WL 2465906 (D. Ariz. Sept. 6, 2005)

Symantec Internet Security Threat Report (Marzo 2007), Volume XI

The Information Assurance Advisory Council (2002), "Engaging the Board: Corporate Governance and Information Risk"

WOLF, Christopher (2006), "Consolidated Case Dismissed When Arbitration Clauses Presented", 183 N.J.L.J. 1166, No. 13.

WORTHY, John (2007), "Denial-of-Service: Plugging the Legal Loopholes?", CLSR 2 3