Deloitte.

**Boletín de Gobierno Corporativo | Otoño 2015**

# La perspectiva del Consejo en el manejo de las crisis cibernéticas

### Olvídese de ser un observador

El rol principal del Consejo de Administración en la organización quizá es el de la supervisión y vigilancia, sin embargo, los consejeros están siendo cada vez llevados de esta posición a atender los problemas cibernéticos. La posibilidad de ser personalmente propenso en el caso de una violación es motivo para estar alerta. Otro problema es el efecto domino que causa una crisis cibernética dentro de la organización. Una cosa es que se caiga el servidor de la empresa y otra, el que se venga abajo la compañía.

Las consecuencias de violaciones al sistema incluyen principalmente costosos e interminables litigios, molestas actividades regulatorias, interrupciones continuas a la operación, ejecución desalineada de la estrategia y aumento en los riesgos de la empresa, todo lo cual disminuye el valor corporativo de la misma.

### Más allá del negocio: esto es personal

El riesgo reputacional para los miembros del Consejo es alto. Los accionistas han respondido a ciertas violaciones cibernéticas pidiendo la remoción de algunos miembros del Consejo o presentando demandas en contra de consejeros y directivos, argumentando conducta indebida e incumplimiento al deber fiduciario, ambas acciones antes o después de la transgresión cibernética. Los miembros del Consejo de compañías que han estado envueltas en incidentes cibernéticos pueden verse afectados en su reputación y eficiencia, mientras que continúa el escrutinio y la atención del incidente.

Las demandas colectivas se han vuelto más comunes como respuesta al quebrantamiento de la seguridad cibernética. Independientemente del resultado de una demanda, los honorarios legales externos e internos necesarios durante el proceso, hacen que éstas resulten muy costosas.

### Amenazas a la capacidad de operación de la empresa.

Más allá de una amenaza personal, los miembros del Consejo de Administración tienen también que contener las formas en

que una falla puede desencadenar una perturbación mayor, más allá del punto inicial de ataque, que a su vez, pueda magnificar las pérdidas.

Considere la estrecha integración del manejo de la demanda en las cadenas de suministro. La misma funcionabilidad cibernética que permite la eficiencia a lo largo de la cadena, -desde el suministro de materia prima para producir hasta los inventarios y la distribución- también genera vulnerabilidad en cada uno de los eslabones de la cadena. Un hackeo que haga caer una pieza vital del equipo, algunas veces por solo unas pocas horas, puede ocasionar una reacción en cadena. Las fallas en la obtención de datos impiden la producción, lo cual puede disminuir los inventarios y resultar en la inhabilidad de completar las órdenes. Cada eslabón en la cadena detenido puede incrementar las pérdidas financieras.

### Crecimiento con compromiso

Las fusiones y adquisiciones, así como las alianzas estratégicas pueden ser particularmente vulnerables a las crisis cibernéticas. El espionaje cibernético en estas negociaciones se ha vuelto común. Se realizan ciberataques con el objetivo de obtener información financiera u operacional para usarla como ventaja competitiva en las transacciones. Los problemas cibernéticos también son utilizados como una forma de devaluar a la compañía exponiendo la debilidad de su seguridad y las fallas que lleven a riesgos.

### Riesgos de relación

La estrecha relación que muchas empresas tienen con sus proveedores y/o distribuidroes quiere decir que éstas son susceptibles de riesgos por parte de los terceros interesados. Dichos ataques pueden penetrar rápidamente dentro de la organización y pueden comprometer las operaciones y crear problemas de deudas.

Una brecha de un tercero puede rápidamente incrustarse en las cuatro paredes de la organización para comprometer las operaciones y crear un tema de responsabilidad. Visto desde la perspectiva del tercero, una brecha o inadecuada salvaguarda en una organización pueden derivar en la pérdida de proveedores, ya que éstos no querrán hacer negocios, temiendo al riesgo de fallas en la organización.

### Más allá del litigio – implicaciones con los seguros

Las violaciones cibernéticas han planteado un nuevo daño que los Consejos de Administración usualmente fallan en considerar: el efecto sobre los seguros. Algunas compañías y sus consejeros se sienten cómodos al tener un seguro que cubra las responsabilidades por violaciones cibernéticas. Las pólizas por filtración de información o de seguridad cibernética se están convirtiendo en una parte importante de los programas de prevención de las compañías. En 2013, sólo el 10 por ciento de los encuestados mencionó que su empresa había adquirido una póliza. En 2014, el porcentaje fue más del doble, creciendo hasta un 26%.  Sin embargo, los proveedores de seguros, se han centrado cada vez más en examinar la raíz de este tipo de violaciones a la seguridad. En caso de que se descubra que las empresas han descuidado sus defensas o no han seguido las mejores prácticas para hacerlo, los pagos por parte del seguro podrían reducirse o incluso ser declinados.

### Un triple enfoque

El Consejo de Administración tiene un papel importante en ayudar a la organización a determinar cómo responder ante el nuevo panorama de amenazas cibernéticas. Los Consejos deben demandar a la administración el evaluar la posición de la empresa en temas de seguridad cibernética y revisar de manera crítica sus capacidades para el manejo de una crisis de este tipo. La gestión de crisis se inicia con la identificación y preparación de los riesgos ante un incidente cibernético que puede convertirse en una crisis y la construcción de un amplio portafolio de capacidades, tales como el monitoreo de eventos, la planeación y simulación de una crisis, la respuesta en tiempo real y la comunicación sobre la crisis. Aunque el número de empresas que tienen planes de respuesta a la violación de datos está creciendo, más de una cuarta parte (27% ) de las empresas aún no tienen un plan implementado.

Estar preparado va más allá de un checklist o de pasar un examen; se requiere conocer dónde están los activos más valiosos de la empresa y de qué forma los criminales podrían tratar de comprometerlos. La gestión

de riesgos cibernéticos comienza asegurando los activos que se encuentran expuestos al riesgo. Si los activos principales de la organización no se protegen adecuadamente, estarán expuestos a riesgos que pueden convertirse en una amenaza mayor de crisis empresarial. En este punto, la gestión del riesgo cibernético se convierte en la gestión de crisis cibernéticas. Con el fin de estar preparadas para una crisis, las organizaciones deben monitorear las amenazas latentes y contar tan pronto como sea posible, con resiliencia en la recuperación ante una crisis.

Monitorear significa que una organización está en una mejor posición para predecir y prevenir los incidentes de seguridad; su enfoque va hacia la inteligencia cibernética que identifica amenazas específicas del entorno de la organización y su continua evolución. El peligro para la inteligencia y la prevención cibernética debe enfatizarse todos los niveles de la organización. De hecho, muchas de las violaciones a la seguridad provienen de correos electrónicos que el personal abre e inadvertidamente filtra el código malicioso en ambiente tecnológico de la empresa.

La resiliencia es clave en caso de una violación; las organizaciones deben responder con rapidez para contener el incidente y evitar su propagación. Mientras que la resiliencia requiere de inversión en modelos de redundancia basada en la tecnología tradicional y las capacidades de recuperación de desastres, el panorama general de la resiliencia incluye también un amplio conjunto de capacidades de gestión de crisis cibernética. Aquí es donde se ponen a prueba los planes, en este momento, la respuesta a los incidentes se utiliza para analizar la amenaza, detener el daño y mitigar cualquier secuela que pudiera presentarse.

El Consejo debe retar a la administración para confirmar que la organización es proactiva, que entiende con claridad la efectividad de su programa de seguridad cibernética, y que su perspectiva se enfoca en los objetivos adecuados tales como:

1. Conocer sus activos más valiosos: No sólo los que quieren proteger, si no los que se necesitan proteger.
2. Conocer a sus aliados: Los contratistas, vendedores y proveedores pueden ser aliados en seguridad y responsabilidades.
3. Hacer del conocimiento una prioridad: Dentro de cada departamento interno y entre los socios externos.
4. Fortalecer y monitorear: Diligentemente reunir la inteligencia; desarrollar el conocimiento situacional; construir, mantener y monitorear proactivamente las defensas.
5. Prepararse para lo inevitable: Probar su proceso de manejo de incidentes.

## Cómo empezar

### Comprométase a evolucionar

El Consejo se debe hacer responsable de implementar un plan de manejo de crisis cibernética y de construir capacidades de resiliencia que aborden los riesgos únicos y propios de la organización. Además, el plan debería medirse regularmente para comprobar su eficacia y buscar una mejora continua, ya que los ciberataques están en constante evolución y el Consejo debe asegurarse que la organización puede también evolucionar.

### Pruebe las capacidades y aprenda de los resultados

Para poder ser eficaces durante un ciberataque, el Consejo debe asegurarse de que la respuesta a incidentes cibernéticos sea probada y que demuestre ser eficaz ante un ataque simulado. Los resultados de las simulaciones deben ser utilizados para corregir las deficiencias en materia de seguridad, vigilancia y capacidad de recuperación.

### No intente hacer esto solo

El Consejo debe garantizar que su organización esté preparada para hacer frente a los problemas a través de diversos expertos que pueden entrar al campo tan pronto como la seguridad se vea comprometida. Un equipo externo puede organizar el caos y mantener a su equipo de gestión centrado en el manejo del negocio.

El equipo debe incluir no sólo especialistas cibernéticos, sino también expertos en relaciones públicas, abogados y otros profesionales que permitan a la organización actuar rápidamente ante las consecuencias de una violación. Una práctica emergente consiste en que los consejeros inviten a expertos en materia de ciber-seguridad para

proporcionar al Consejo, asesoría u otra perspectiva del tema.

### La gestión de crisis cibernética en acción

#### Cinco prioridades clave

En un esfuerzo liderado por la preocupación del Consejo de Administración de enfrentar crisis potenciales de seguridad, una empresa global de energía adoptó la seguridad cibernética como una de sus cinco prioridades. El Consejo se encargó de buscar un asesor de seguridad quien expondría las amenazas específicas de la organización.

Después, el Consejo solicitó el liderazgo de los directivos para abordar la estrategia cibernética de la empresa, lo que llevó al desarrollo de un enfoque integral y coordinado de la organización.

Los requerimientos de la seguridad cibernética en cada unidad de negocio se alinearon de acuerdo a los estándares de la industria y las mejores prácticas, pero lo más importante, en proporción a las amenazas reales que éstas enfrentan en la actualidad.

## Mayor información

**Daniel Aguiñaga**
Socio Gobierno Corporativo
Tel: +52 (55) 5080-6000
**daguinaga@deloittemx.com**

**Visite Deloitte México**
**www.deloitte.com/mx**

**Gobierno Corporativo**
**www.deloitte.com/mx/gobiernocorporativo**

**Aguascalientes**
Universidad 1001, piso 12-1, Bosques del Prado
20127 Aguascalientes, Ags.
Tel: +52 (449) 910 8600, Fax: +52 (449) 910 8601

**Cancún**
Avenida Bonampak SM 6, M 1, lote 1, piso 10
77500 Cancún, Q. Roo
Tel: +52 (998) 872 9230, Fax: +52 (998) 892 3677

**Chihuahua**
Av. Valle Escondido 5500, Fracc. Des. El Saucito E-2, piso 1,
31125 Chihuahua, Chih.
Tel: +52 (614) 180 1100, Fax: +52 (614) 180 1110

**Ciudad Juárez**
Baudelio Pelayo No. 8450
Parque Industrial Antonio J. Bermúdez
32400 Ciudad Juárez, Chih.
Tel: +52 (656) 688 6500, Fax: +52 (656) 688 6536

**Culiacán**
Calz. Insurgentes 847 Sur, Local 103, Colonia Centro Sinaloa
80128 Culiacán, Sin.
Tel: +52 (667) 761 4339, Fax: +52 (667) 761 4338

**Guadalajara**
Avenida Américas 1685, piso 10, Colonia Jardines Providencia
44638 Guadalajara, Jal.
Tel: +52 (33) 3669 0404, Fax: +52 (33) 3669 0469

**Hermosillo**
Blvd. Francisco E. Kino 309-9, Colonia Country Club
83010 Hermosillo, Son.
Tel: +52 (662) 109 1400, Fax: +52 (662) 109 1414

**León**
Paseo de los Insurgentes 303, piso 1, Colonia Los Paraísos
37320 León, Gto.
Tel: +52 (477) 214 1400, Fax: +52 (477) 214 1405

**Mazatlán**
Avenida Camarón Sábalo 133, Fraccionamiento Lomas
de Mazatlán
82110 Mazatlán, Sin.
Tel: +52 (669) 989 2100, Fax: +52 (669) 989 2120

**Mérida**
Calle 56 B 485 Prol. Montejo Piso 2
Colonia Itzimna 97100 Mérida, Yuc.
Tel: +52 (999) 920 7916, Fax: +52 (999) 927 2895

**Mexicali**
Calzada Francisco López Montejano 1342, Piso 7 Torre Sur
Fraccionamiento esteban cantú
21320 Mexicali, B.C.
Tel: +52 (686) 905 5200, Fax: +52 (686) 905 5232

**México, D.F.**
Paseo de la Reforma 489, piso 6, Colonia Cuauhtémoc
06500 México, D.F.
Tel: +52 (55) 5080 6000, Fax: +52 (55) 5080 6001

**Monclova**
Blvd. Ejército Nacional 505, Colonia Los Pinos
25720 Monclova, Coah.
Tel: +52 (866) 635 0075, Fax: +52 (866) 635 1761

**Monterrey**
Lázaro Cárdenas 2321 Poniente, PB, Residencial San Agustín
66260 Garza García, N.L.
Tel: +52 (81) 8133 7300, Fax: +52 (81) 8133 7383

Carr. Nacional 85, 5000, local S-6 Colonia La Rioja
64988, monterrey, N.L.
Tel. +52 (631) 320 1673
Fax: +52 (631) 320 1673

**Nogales**
Apartado Postal 384-2
Sucursal de Correos “A”
84081 Nogales, Son.
Tel: +52 (631) 320 1673, Fax: +52 (631) 320 1673

**Puebla**
Edificio Deloitte, Vía Atlixcayotl 5506, piso 5, Zona Angelópolis
72190 Puebla, Pue.
Tel: +52 (222) 303 1000, Fax: +52 (222) 303 1001

**Querétaro**
Avenida Tecnológico 100-901, Colonia San Ángel
76030 Querétaro, Qro.
Tel: +52 (442) 238 2900, Fax: +52 (442) 238 2975, 238 2968

**Reynosa**
Carr. Monterrey-Reynosa 210-B, PA
Fracc. Portal San Miguel
88730 Reynosa, Tamps.
Tel: + 52 (899) 921 2460, Fax: +52 (899) 921 2462

**San Luis Potosí**
Av. Salvador Nava Martínez 3125, 3-A
Fracc. Colinas del Parque
78294 San Luis Potosí, S.L.P.
Tel: +52 (444) 1025300, Fax: +52 (444) 1025301

**Tijuana**
Misión de San Javier 10643, Piso 8,
Zona Urbana Rio Tijuana. Tijuana B.C., 22010
Tel: +52 (664) 622 7878, Fax: +52 (664) 681 7813

**Torreón**
Independencia 1819-B Oriente, Colonia San Isidro
27100 Torreón, Coah.
Tel: +52 (871) 747 4400, Fax: +52 (871) 747 4409

# deloitte.com/mx