Cinco prácticas recomendadas de gobierno para la seguridad de la información

En 2015 se divulgaron más de 169 millones de registros personales debido a más de 700 filtraciones cometidas en el ámbito financiero, empresarial, educativo, gubernamental y sanitario.

INTRODUCCIÓN

La información está por todas partes: en dispositivos móviles, en la nube, circulando de un lado para otro. Cada vez hay más información y son más las empresas las que utilizan dicha información para perfeccionar sus prácticas, ya que ésta proviene de diferentes plataformas y se puede encontrar en diferentes formatos. El aumento de información, las nuevas tecnologías y las amenazas cibernéticas continuas suponen un problema para las empresas, que tienen que establecer una serie de estrategias, marcos y políticas para mantener a salvo dicha información.

Las amenazas aumentan y evolucionan rápidamente, ya que los delincuentes han descubierto nuevas formas de sortear dicha protección y conseguir esa valiosa información. Según el informe sobre filtración de datos del ITRC[1], en 2015 se divulgaron más de 169 millones de registros personales, debido a más de 700 filtraciones cometidas en el ámbito financiero, empresarial, educativo, gubernamental y sanitario.

El IT Governance Institute[2] define el gobierno para la seguridad de la información como “un subconjunto de gobierno empresarial que ofrece una dirección estratégica, asegura que se logran los objetivos, gestiona los riesgos y hace uso de la responsabilidad de recursos de la empresa y, además, gestiona el éxito o el fracaso del programa de seguridad de la empresa”.

En general, el gobierno para la seguridad de la información exige una estructura organizativa, la asignación de funciones y responsabilidades, así como medidas y tareas establecidas, todo ello estratégicamente desarrollado y definido por el Consejo de Administración y la Dirección Ejecutiva.

Diligent

"¿Cómo utiliza de forma efectiva una empresa sus recursos para alcanzar un nivel aceptable en lo que respecta a la seguridad cibernética, así como para minimizar los riesgos?" pregunta un artículo de la revista Bloomberg Government[3]. Es una pregunta que solo pueden resolver los responsables en la toma de decisiones del Consejo de Administración.

Este documento tiene como objetivo ofrecer prácticas recomendadas y una serie de directrices para aplicar con éxito, el gobierno para la seguridad de la información, además de responder las siguientes preguntas:

- ¿Cómo se define el gobierno para la seguridad de la información?
- ¿Cuáles son las ideas equivocadas sobre el gobierno para la seguridad de la información?
- ¿Por qué es importante el gobierno para la seguridad de la información?
- ¿Quién es el responsable del gobierno para la seguridad de la información?

QUÉ NO SE CONSIDERA GOBIERNO PARA LA SEGURIDAD DE LA INFORMACIÓN

No se debe confundir el gobierno para la seguridad de la información con la gestión de la TI, que se centra básicamente en tomar decisiones tácticas para disminuir los riesgos de seguridad.

Piense en gobierno al determinar quién está autorizado y es responsable de tomar esas decisiones relacionadas con la seguridad. No se trata de la aplicación de la política, sino del control y la creación del programa. No se trata del cumplimiento de la política (declaración de principios y funciones de gestión de TI), sino de establecer la política de seguridad. En definitiva, el gobierno para la seguridad de la información se centra en la estrategia, no en el plan estratégico.

¿POR QUÉ ES IMPORTANTE EL GOBIERNO PARA LA SEGURIDAD DE LA INFORMACIÓN?

El gobierno para la seguridad de la información tiene como objetivo establecer medidas estratégicas para proteger la información de una empresa, que puede integrar datos e información extremadamente confidenciales de carácter financiero, jurídico, de clientes, de socios, de investigación, de desarrollo y de propiedad exclusiva, entre otros. Las empresas cada vez cuentan con más información que podría ser de gran valor para los competidores y, lo que es peor, para los delincuentes.

Durante estos años, los delincuentes cibernéticos han sido noticia por pirateo y filtración de información de gran repercusión mediática. Desde el pirateo contra Sony Pictures Entertainment, donde los delincuentes robaron unos 100 terabytes de información confidencial[4], hasta la filtración de información de Anthem Medical[5], todos los sectores pueden sufrir este tipo de ataques. La filtración de información puede tener efectos dañinos incluso mucho después de que se produzca: responsabilidades legales, daño a la reputación de la marca, falta de confianza por parte de los clientes y de los socios, así como una disminución de los ingresos. Según un estudio de Ponemon[6] de 2016, el coste medio por filtración de información es de 4 millones de dólares estadounidenses.

El gobierno estratégico para la seguridad de la información reviste gran importancia a la hora de que las empresas garanticen a sus clientes, socios y empleados, que están trabajando con una empresa segura. Debido a que os empleados pueden acceder a los datos corporativos cada vez con mayor asiduidad, a través de los dispositivos móviles y de la nube, es importante que las empresas lleven a cabo prácticas de seguridad para garantizar que son los empleados apropiados quienes tienen acceso a la información y, por supuesto, para asegurarse de que los delincuentes no accedan a esta información confidencial.

¿QUIÉN ES EL RESPONSABLE DEL DESARROLLO DEL GOBIERNO PARA LA SEGURIDAD DE LA INFORMACIÓN?

Mientras que la seguridad debe ser competencia de todos los equipos y empleados, el equipo directivo es responsable de establecer y mantener un marco para el gobierno para la seguridad de la información. Ya sea el Consejo de Administración, la dirección ejecutiva, o un comité directivo (o todos ellos), el gobierno para la seguridad de la información requiere un plan estratégico y una toma de decisiones.

CINCO PRINCIPALES PRÁCTICAS RECOMENDADAS DE GOBIERNO PARA LA SEGURIDAD DE LA INFORMACIÓN

A continuación, se muestra una serie de soluciones estratégicas para una situación más favorable en la empresa respecto al gobierno para la seguridad de la información:

1. Adoptar un enfoque holístico de la estrategia: Antes de aplicar el gobierno para la seguridad de la información, analice detenidamente de qué manera puede influir la seguridad en su empresa. Una encuesta a nivel de toda la empresa puede ayudarle a saber qué datos hay que proteger. También puede ayudar a conseguir que las principales partes interesadas compren la iniciativa. Algunos de los aspectos a tener en cuenta son:

- ¿Qué datos hay que proteger?
- ¿Cuáles son los riesgos?
- ¿Qué políticas estratégicas se deben formular?
- ¿Qué equipos deben ser responsables de llevar a cabo estas políticas?

La estrategia de seguridad también implica adaptarse e involucrarse en los objetivos de la TI y de la empresa. Obtenga información de todas las partes interesadas de la empresa (TI, ventas, marketing, departamento jurídico y de operaciones) para entender sus preocupaciones y problemas, así como para valorar sus habilidades y su experiencia.

Evite soluciones modelo y trabajar en compartimentos aislados, que pueden suponer más obstáculos y soluciones de seguridad dispersas fragmentadas. Un enfoque holístico asegura que el equipo directivo (los creadores del gobierno para la seguridad de la información) obtiene más niveles de control y visibilidad.

2. Fomentar la sensibilización y la formación en la empresa: Establecer un gobierno para la seguridad de la información para luego no continuar, puede acarrear resultados negativos, como un rechazo a su adopción, una mala interpretación de políticas, funciones y responsabilidades, así como vulnerabilidades en la seguridad. La continua adaptación al gobierno para la seguridad requiere concienciación, educación y formación para todos aquellos que estén involucrados.

La seguridad no solo supone un problema para la TI. Es responsabilidad de todos.

- ¿Sus empleados llevan dispositivos personales al trabajo?
- ¿Utilizan aplicaciones homologadas?
- ¿Cuál es su actitud al gestionar información confidencial de la empresa?

La realización asidua de encuestas a nivel empresarial, los seminarios de seguridad y la formación sobre prácticas recomendadas de seguridad son formas de concienciar a los empleados de la importancia de la seguridad.

Aunque el Consejo de Administración, la Junta Directiva, La Dirección Ejecutiva y el Comité Directivo elaboren el gobierno para la seguridad de la información, éste es competencia de todos los empleados de la empresa. El gobierno crea políticas y asigna responsabilidades, pero cada miembro es responsable de seguir las normas de seguridad.

Debe mantenerse siempre la concienciación, formación y educación de unas prácticas recomendadas de seguridad. Por ejemplo, una empresa puede enviar a determinados miembros del equipo a conferencias formativas de seguridad para que conozcan las últimas técnicas del sector. Gracias a esas nuevas perspectivas, estas personas pueden compartir sus conocimientos con toda la empresa.

3. Controlar y evaluar: El gobierno para la seguridad de la información requiere una constante valoración y evaluación.

- ¿Qué políticas funcionan?
- ¿Cuáles no?
- ¿Qué equipos o personas no están siguiendo las políticas de seguridad?
- ¿La cantidad de incidentes de seguridad está afectando a la reputación con los clientes y socios?

Medir el rendimiento de los esfuerzos realizados en lo que respecta al gobierno para la seguridad de la información asegura que se están cumpliendo los objetivos y que los recursos se están gestionando de manera apropiada.

- ¿Con qué frecuencia analiza sus medidas de seguridad?
- ¿Con qué frecuencia se produce la filtración de información?
- ¿Cuál es el tiempo de respuesta ante los incidentes?
- ¿Qué políticas de seguridad funcionan y cuáles no?

Por ejemplo, una empresa puede realizar, a modo de prueba, filtraciones de información para comprobar cómo actúan los equipos. Los resultados pueden mostrar los aspectos sobre los que la empresa debe trabajar, así como los que ya tienen identificados.

4. Fomentar la comunicación abierta entre todas las partes interesadas: Es muy importante que las partes interesadas sientan que pueden comunicarse directamente con el equipo directivo. Trabajar en compartimentos aislados puede crear

cierta confusión acerca de la comunicación importante sobre el gobierno de la seguridad.

Si se produce filtración de la información, ¿los empleados de cualquier nivel de la empresa deben comunicárselo con total libertad al equipo directivo? O, ¿deben intentar no transmitir ese tipo de noticias?

La comunicación abierta fomenta la confianza a la vez que aumenta la visibilidad en toda la empresa. Para un mayor compromiso, piense en crear un comité directivo compuesto por la dirección ejecutiva y consejeros del equipo principal para revisar y evaluar los riesgos actuales de seguridad. Los miembros deben ser consejeros de los siguientes departamentos: TI, financiero, RR.PP., marketing, jurídico y de operaciones. Las reuniones regulares del comité directivo pueden asegurar que existe una fidelidad constante a las políticas de seguridad. Por ejemplo, si se crea una nueva política de seguridad, los consejeros del departamento, que forman parte del comité directivo, pueden asegurar que sus equipos ponen en marcha la política.

5. Promover la agilidad y la adaptabilidad: El panorama digital está evolucionando rápidamente a medida que las nuevas plataformas afectan a la forma en la que hacemos negocios. Su gobierno para la seguridad de la información, además de establecer sólidas políticas y directrices, debe estar abierto a la adaptación. Una empresa debe gestionar y medir la fuerza global de las políticas de seguridad. Algunas de las preguntas a tener en cuenta son:

- ¿Qué funciona?
- ¿Qué no funciona?
- ¿Qué podemos cambiar?

Por ejemplo, un empleado del departamento de seguridad de TI debe tener la suficiente experiencia y conocimientos en cuanto a efectividad de una determinada política de seguridad. Si el consejero está dispuesto a escuchar los comentarios y sugerencias de los miembros del equipo, estos cambios se tendrían que realizar rápidamente.

CONCLUSIÓN

El gobierno para la seguridad de la información no surge de la noche a la mañana: es un proceso continuo de aprendizaje, revisión y adaptación. Mientras que cada empresa puede tener sus propias necesidades específicas, asegurar su información es un objetivo común para todas las empresas. Las tecnologías emergentes y las amenazas cibernéticas seguirán apareciendo. Seguirá habiendo filtración de información y produciéndose incidentes relacionados con la seguridad. En lugar de estipular una codificación cuando se produzca filtración de la información, las empresas deben plantearse el gobierno para la seguridad de la información. El objetivo para todas las empresas debe ser el de ofrecer una seguridad de la información y reducir los impactos negativos, así como los riesgos, a un nivel aceptable. Seguirá habiendo amenazas y produciéndose incidentes, pero un plan de gobierno para la seguridad de la información, fortalecerá la seguridad de su empresa al mismo tiempo que protegerá esa valiosa información.

FUENTES:

1. "Data Breach Reports," ITRC, 29 de diciembre de 2015, http://www.idtheftcenter.org/images/breach/ DataBreachReports_2015.pdf
2. "Information Security Governance: Guidance for Boards of Directors and Executive Management" 2ª edición, IT Governance Institute, 2006, http://www.isaca.org/knowledge-center/research/documents/information-security- govenance-for-board-of-directors-and-executive-management_res_eng_0510.pdf
3. "Why cyber is a boardroom issue," Tom Skypek, 21 de abril de 2016 Bloomberg Government, http://about.bgov.com/blog/why-cyber-is-a-boardroom-issue/
4. "The Sony Hackers Still Have A Massive Amount of Data that Hasn't Been Leaked Yet," Business Insider, James Cook, 16 de diciembre de 2014, http://www.businessinsider.com/the-sony-hackers-still-have-a-massive-amount-of- data-that-hasnt-been-leaked-yet-2014-12
5. "Insurance Giant Anthem Hit by Massive Data Breach," CNN Money, Charles Riley, 4 de febrero de 2015, http://money.cnn.com/2015/02/04/ technology/anthem- insurance-hack-data-security/
6. "2016 Cost of Data Breach Study," Estudio Ponemon de 2016, http://www-03.ibm.com/security/data-breach/