Las cinco mejores prácticas para la gobernanza de la seguridad de la información

En 2015 se expusieron más de 169 millones de registros personales, como resultado de más de 700 filtraciones públicamente conocidas que tuvieron lugar en los sectores financiero, empresarial, educativo, gubernamental y de cuidado de salud.

INTRODUCCIÓN

Los datos están en todas partes, en dispositivos móviles, en la nube, en tránsito. La acumulación de datos y el aumento de negocios que emplean datos para afinar mejor sus prácticas están evolucionando rápidamente ya que los datos vienen de diversas plataformas y en diferentes formatos. El crecimiento de los datos, las nuevas tecnologías y las cambiantes amenazas informáticas crean desafíos para las organizaciones que buscan establecer las estrategias, la estructura y las políticas para preservar la seguridad de toda esa información.

Las amenazas aumentan y evolucionan rápidamente a medida que los delincuentes descubren nuevas maneras de eludir defensas y llegar a datos valiosos. En 2015, se expusieron más de 169 millones de registros personales como resultado de más de 700 filtraciones públicamente conocidas que tuvieron lugar en los sectores financiero, empresarial, educativo, gubernamental y de cuidado de salud, de acuerdo con el Informe de las investigaciones sobre Violaciones de la Información del ITRC[1].

El IT Governance Institute[2] define la Gobernanza de la seguridad de la información como “un subconjunto de la gobernanza empresarial que proporciona dirección estratégica, garantiza que se alcancen los objetivos, maneja riesgos y usa responsabilidad de recursos de la organización, y supervisa el éxito o fracaso del programa de seguridad empresarial”.

En general, la gobernanza de la seguridad de la información requiere de una estructura

Diligent

organizativa, la asignación de roles y responsabilidades, así como de mediciones y tareas definidas; todo desarrollado estratégicamente y definido por la junta directiva y la gerencia ejecutiva.

"¿Cómo despliega una empresa sus recursos de la manera más efectiva para disminuir los riesgos de seguridad informática a un nivel aceptable?" es la pregunta que formula un artículo de la revista Bloomberg Government[3]. Esa es una pregunta que solo pueden responder los responsables de la toma de decisiones a nivel de la junta directiva.

Este documento tiene el objetivo de proporcionar mejores prácticas y lineamientos para implementar exitosamente una gobernanza de seguridad de la información estratégica, así como de responder a las siguientes preguntas:

- ¿Cómo se define la gobernanza de la seguridad de la información?
- ¿Cuáles son los conceptos erróneos sobre la gobernanza de la seguridad de la información?
- ¿Por qué es importante la gobernanza de la seguridad de la información?
- ¿Quién es responsable de la gobernanza de la seguridad de la información?

LO QUE NO ES LA GOBERNANZA DE LA SEGURIDAD DE LA INFORMACIÓN

La gobernanza de la seguridad de la información no se debe confundir con la administración de TI, la cual se preocupa principalmente por tomar decisiones tácticas para mitigar riesgos de seguridad.

Piense en la gobernanza como en la determinación de quién está autorizado para y es responsable de tomar las decisiones relacionadas con la seguridad. No es la implementación de la política, sino la supervisión y creación del programa. No es la aplicación de la política (estatuto de la administración de TI), sino la promulgación de la política de seguridad. En pocas palabras, el gobernanza de la seguridad de la información se enfoca en la estrategia, no en la táctica.

¿POR QUÉ ES IMPORTANTE LA GOBERNANZA DE LA SEGURIDAD DE LA INFORMACIÓN?

La gobernanza de la seguridad de la información tiene como objetivo establecer medidas estratégicas para proteger la información de una organización, la cual puede constar de datos e información altamente confidenciales: información financiera, legal, de clientes, socios, investigación y desarrollo, propiedad y más. Las organizaciones mantienen más y más datos que podrían ser valiosos para competidores, o peor, delincuentes.

En años recientes, los delincuentes informáticos han protagonizado titulares con ataques de alto perfil y filtraciones de datos. Desde el ataque a Sony Pictures Entertainment, en el que delincuentes robaron un estimado de 100 terabytes de datos confidenciales[4], hasta la filtración de datos de Anthem Medical[5], todas las industrias son vulnerables a un ataque. Una filtración de datos puede tener efectos dañinos incluso tiempo después del incidente: responsabilidades legales, daños a la reputación de la marca, falta de confianza de los clientes y socios y descensos en los ingresos asociados. De acuerdo a un estudio de Ponemon de 2016[6], el costo promedio de una filtración de datos es $4 millones.

Una gobernanza estratégica de la seguridad de la información es vital para que todas las organizaciones le aseguren a sus clientes, socios y empleados que están trabajando con una empresa segura. Ya que los datos corporativos se vuelven más accesibles para los empleados a través de dispositivos móviles y la nube, es importante que las empresas mantengan actualizadas las prácticas de seguridad para garantizar que los empleados adecuados tengan acceso a esos datos. Y, por supuesto, para asegurarse de que los delincuente no tengan acceso a datos confidenciales.

¿QUIÉN ES RESPONSABLE DE DESARROLLAR LA GOBERNANZA DE LA SEGURIDAD DE LA INFORMACIÓN?

Aunque la seguridad debe ser una preocupación para todos los equipos y empleados, el liderazgo es responsable de establecer y mantener una estructura para la gobernanza de la seguridad de la información. Independientemente de que sea la junta directiva, gerencia ejecutiva o un comité directivo — o todos estos — la gobernanza de la seguridad de la información requiere planificación estratégica y toma de decisiones.

LAS CINCO MEJORES PRÁCTICAS PARA LA GOBERNANZA DE LA SEGURIDAD DE LA INFORMACIÓN

A continuación encontrará soluciones estratégicas que le permitirán a una organización lograr una exitosa gobernanza de la seguridad:

1. Adoptar un enfoque global de estrategia: Antes de implementar una gobernanza de la seguridad de la información, observe en general cómo la seguridad afecta a su organización. Una encuesta en la empresa puede ayudar a detectar cuáles datos necesitan protección. Esto también puede ayudar a conseguir un compromiso rápido de las partes interesadas

claves. Las preguntas que se deben responder incluyen:

- ¿Cuáles datos necesitan protección?
- ¿Cuáles son los riesgos?
- ¿Cuáles políticas estratégicas se deben crear?
- ¿Cuáles equipos deben ser responsables de llevar a cabo estas políticas?

La estrategia de seguridad también se trata de alinearse y conectarse con negocios y objetivos de TI. Obtenga la opinión de todas las partes interesadas en toda la organización, a partir de los departamentos de TI, ventas, marketing, operaciones y legales, para comprender sus preocupaciones y desafíos, así como para evaluar sus habilidades y experiencia.

Evite soluciones para eliminar los cookies y el trabajo en silos, lo cual puede crear más obstáculos y soluciones de seguridad desiguales y fragmentadas. Un enfoque global asegura que el liderazgo — los creadores de la gobernanza de la seguridad de la información — obtengan más niveles de control y visibilidad.

2. Crear conciencia y capacitación en toda la organización: Establecer una gobernanza de seguridad de la información y posteriormente desatenderla puede traer resultados negativos, como falta de adopción, incomprensión de políticas, roles y responsabilidades, y vulnerabilidades de seguridad. La adherencia continua a la gobernanza de la seguridad requiere conciencia, educación y capacitación para todos los involucrados.

La seguridad no es solo una preocupación para TI. Es responsabilidad de todos.

- ¿Traen sus empleados sus propios dispositivos al trabajo?
- ¿Usan aplicaciones aprobadas?
- ¿Cuáles son sus actitudes para manejar los datos confidenciales de la empresa?

Encuestas frecuentes en toda la empresa, seminarios de seguridad y educación sobre mejores prácticas de seguridad son maneras de hacer que todos los empleados siempre tengan en cuenta la seguridad.

Aunque sea desarrollado por la junta directiva, gerencia ejecutiva o comités directivos, la gobernanza de la seguridad de la información es para todos los empleados de la organización. La gobernanza crea políticas y asigna responsabilidades, pero cada miembro es responsable de seguir las normas de seguridad.

La concienciación, capacitación y educación sobre las mejores prácticas de seguridad deben ser continuas. Por ejemplo, una organización puede enviar a miembros específicos de un equipo a conferencias de capacitación en seguridad para que aprendan las técnicas más recientes de la industria. Con los nuevos conocimientos adquiridos, estas personas pueden luego compartir sus opiniones con el grueso de la organización.

3. Supervisar y medir: La gobernanza de la seguridad de la información requiere evaluación y medición constantes.

- ¿Cuáles políticas funcionan?
- ¿Cuáles políticas no funcionan?
- ¿Cuáles equipos o personas no siguen las políticas de seguridad?
- ¿La cantidad de incidentes de seguridad está afectando la reputación ante clientes y socios?

Medir el rendimiento de los esfuerzos de la gobernanza de la seguridad de la información garantiza que los objetivos se alcancen y que los recursos se administren apropiadamente.

- ¿Con qué frecuencia lleva a cabo pruebas de sus medidas de seguridad?
- ¿Con qué frecuencia ocurren filtraciones de datos?
- ¿Cuál es el tiempo de respuesta a los incidentes?
- ¿Cuáles políticas de seguridad funcionan y cuáles no?

Por ejemplo, una organización podría mantener escenarios simulados de filtración de datos para determinar qué tan bien resisten los equipos. Estos resultados pueden mostrar en qué necesita trabajar una empresa para seguir con su labor y qué han aprendido ya.

4. Fomentar la comunicación abierta entre todas las partes interesadas: Es vital que todas las partes interesadas sientan

que pueden comunicarse directamente con sus líderes. Trabajar en silos crea el riesgo de ensombrecer comunicaciones importantes relacionadas con la gobernanza de seguridad.

Si ocurre una filtración de datos, ¿se sienten los empleados de cualquier nivel de la organización lo suficientemente cómodos para hacérselo saber a los líderes? ¿O intentarán ocultar cualquier noticia negativa a las instancias superiores?

La comunicación abierta promueve la confianza al mismo tiempo que aumenta la visibilidad a lo largo y ancho de la organización. Para mejorar aún más el compromiso, considere crear un comité directivo conformado por la gerencia ejecutiva y líderes de equipo claves para revisar y evaluar riesgos de seguridad actuales. Los miembros pueden incluir líderes de los departamentos de TI, finanzas, RR.PP., marketing, legal y de operaciones. Reuniones regulares del comité directivo pueden asegurar que haya una adherencia continua a las políticas de seguridad. Por ejemplo, si se crea una nueva política de seguridad, líderes de departamento que formen parte del comité directivo, pueden asegurarse de que sus equipos implementen la política.

5. Promover la agilidad y la adaptabilidad: El panorama digital evoluciona rápidamente a medida que nuevas plataformas tienen impacto en la manera en que hacemos negocios. Su gobernanza de la seguridad de la información, al mismo tiempo que establece políticas sólidas y lineamientos, debe estar abierto a la adaptación. Una organización debe supervisar y medir la fortaleza general de las políticas de seguridad. Las preguntas que se deben formular incluyen:

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

Por ejemplo, un empleado en las trincheras de seguridad de TI puede tener experiencia práctica y opiniones sobre la efectividad de una política de seguridad particular. Si los líderes son receptivos a escuchar las opiniones y sugerencias del miembro del equipo, también debe haber la agilidad para hacer esos cambios.

CONCLUSIÓN

Una gobernanza de la seguridad de la información exitosa no llega de la noche a la mañana; es un proceso continuo de aprendizaje, revisión y adaptación. Aunque cada empresa puede tener sus necesidades específicas, asegurar los datos es una meta común para todas las organizaciones. Las tecnologías emergentes y las amenazas informáticas seguirán evolucionando. Las filtraciones de datos y los incidentes de seguridad ocurrirán. En lugar de luchar con una infracción de la seguridad, las organizaciones deben poner una gobernanza de la seguridad de la información proactiva y estratégica al frente. La meta de todas las empresas debe ser proveer seguridad de la información y reducir los impactos adversos y riesgos a un nivel aceptable. Las amenazas y los incidentes ocurrirán, pero con un plan de gobernanza de la seguridad de la información implementado, fortalece la postura de seguridad de su organización mientras protege su 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," 2016 Ponemon Study, http://www-03.ibm.com/security/data-breach/