¿Cómo el espionaje corporativo afecta el horizonte estratégico de las organizaciones, los consumidores y el mercado?

Sebastián Camilo Stave Rodríguez*

RESUMEN

El eslabón más débil de una compañía a la hora de proteger la información son los mismos empleados, ya que se pueden tener los mejores estándares de seguridad para protegerla, pero siempre la información que se quiere proteger está disponible para un grupo de personas; he aquí la importancia de mantener en la organización una baja o nula rotación, siendo esta una herramienta clave para las operaciones de la misma. La seguridad en este ámbito tiene como fin tener un ambiente sano y motivador que ayude a la conservación de la información. Este artículo nos muestra un panorama sobre la importancia de este aspecto hoy en día en las organizaciones.

Palabras clave: Espionaje, Estrategia, Objetivo, Proyectos, Fuga, Información, Competidores, Rentabilidad.

* Estudiante del programa de pregrado en Administración de Empresas.

Un sinnúmero de empresas se han visto obligadas a proteger sus activos de la información, del llamado espionaje corporativo, un acto delictivo judicialmente penalizado por distintas leyes (como "sarbanes-oxley implementada en Estados Unidos"[1]), y a la vez que se aumenta la seguridad a través de distintas medidas ("normas como la ISO 27001"[2], protocolos de seguridad como "PSI-DSS" que se implementa para la protección de las tarjetas de crédito, la circular 052 en Colombia[3], entre otras medidas) en cada país, pese a lo cual "en 1999, las compañías del Ranking Fortune 1000 reportaron un total de 45 billones de dólares en pérdidas debidas al espionaje corporativo" (Trends in Proprietary Information Loss, 1999).

La actual incursión de las tecnologías de la información ha causado que se empeore la situación, debido a que las empresas guardan mucha de su información más importante en medios digitales a los cuales se puede acceder por la red. Pero también existen otros métodos: uno de los principales inconvenientes son los mismos empleados de la empresa, en la medida en que el mismo recurso humano puede ser una de las mayores filtraciones de información en una empresa, lo cual apoya las teorías que buscan unos mejores ambientes laborales (enfoque de las relaciones humanas por Elton Mayo, Teoría Z por William Ouchi) y proteger el recurso humano (en Ecopetrol se preocupan por que sus empleados permanezcan en la empresa, protegiendo el recurso humano para evitar que sus empleados se vayan a otra empresa[4]).

Existen muchos métodos para sustraer información de una empresa, uno de los cuales es la ingeniera social, entendida como "la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Es una técnica que pueden usar ciertas personas, tales como investigadores privados, criminales, o delincuentes computacionales, para obtener información, acceso o privilegios en sistemas de información que les permitan realizar algún acto que perjudique o exponga la persona u organismo comprometido a riesgo o abusos"[5]. Otra forma es con el uso de sobornos, con los cuales las compañías competidoras pretenden sobornar a los empleados de la compañía para que brinden información privada e importante de esta. Pero muchos de estos casos que involucran el personal de las mismas empresas en estas estafas, no suelen salir a la luz pública, por distintas razones, ya sea por evitar desprestigiar las empresas y no dañar su imagen pública y corporativa.

También existen las amenazas externas, principalmente los *hackers*, que intentan quebrantar la seguridad informática de la empresa buscando puntos débiles en ella.

Por tal razón, muchas empresas como Google, protegen sus activos de la información, en grandes centros de alta seguridad a los cuales se les invierten millones de dólares para evitar estas fugas de información.

1 Ley Sarbanes-Oxley [en línea] Wikipedia. 8 de febrero de 2011 [consultado: 9 de marzo de 2011] Disponible en: [http://es.wikipedia.org/wiki/Ley_Sarbanes-Oxley]

2 ISO 27001 [en línea] Bureau Veritas Services [consultado: 9 de marzo de 2011] Disponible en: [http://www.certification.bureauveritas.com.co/dynamicdata/fileupload/ISO_27001.pdf]

3 Inseguridad informática en el sector Bancario [en línea] El Tiempo. 8 de febrero de 2011 [consultado: 9 de marzo de 2011] Disponible en: [http://www.eltiempo.com/participacion/blogs/default/un_articulo.php?id_blog=3516456&id_recurso=400002707]

4 Conferencia dictada en la Universidad Externado de Colombia, por la Jefa de relaciones humanas de Ecopetrol, jueves 3 de marzo de 2011.

5 Ingeniería social (seguridad informática) [en línea] Wikipedia. 12 de febrero de 2011 [consultado: 9 de marzo de 2011] Disponible en: [http://es.wikipedia.org/wiki/Ingenier%C3%ADa_social_(seguridad_informática)].

Por todo lo anterior, el problema no solo afecta el ámbito competitivo de las empresas, sino también a los empleados que laboran en ellas (sus ambientes laborales), y de una u otra forma esto repercute en los productos del mercado que se les ofrecen a los consumidores. ¿Será esto bueno para los consumidores? ¿Se mantendrá la calidad de los productos? ¿El espionaje corporativo es un acto normal entre organizaciones y de ser así no sería mejor una mutua cooperación entre empresas del mismo sector para alcanzar fines mutuos? ¿Las empresas qué deben hacer para mantener a gusto a los empleados y crear una identidad de familia en la empresa?

Contexto general

La siguiente es un ejemplo de cómo el espionaje corporativo ha llegado a afectar las organizaciones, donde una perspectiva de libre mercado y libre acceso a la información, es la justificación para el robo de información privilegiada y clave de las empresas por parte de los competidores.

"Sus casos ponen al descubierto a una industria global que en un año le ha quitado a las compañías estadounidenses su información privilegiada y su propiedad intelectual por un valor de US$59 billones (£34 billones), según una encuesta de la American Society of Industrial Security (Sociedad Americana de Seguridad Industrial) y Pricewaterhouse Coopers, publicada en el año 2002. Un cálculo estimativo indica que las cifras actuales ascienden a US$100 billones. Este estudio del área, que ha tomado en cuenta las experiencias de 138 compañías pertenecientes al *ranking* Fortune 1000, demostró que el 40% de los empleados sospecha o efectivamente sabe del robo de información privilegiada en sus compañías e informó que la mitad de aquellos que habían sido afectados mencionaron que el blanco del espionaje fueron una serie de proyectos de investigación y desarrollo, con una pérdida promedio de US$405.000 (£231,000) por cada uno de estos robos –la cifra no tuvo en cuenta la ventaja competitiva perdida" (Blogg, *Espionaje corporativo*).

Un problema no tan solo de las empresas

"Una asombrosa estadística muestra que el 90% de las computadoras conectadas a Internet están infectadas con *spyware* –se trata de un *software* instalado en una computadora sin que su dueño lo sepa con el fin de recopilar información y retransmitirla a terceros" (ídem).

El espionaje se encuentra no solo en estas empresas que parecen estar en una realidad más allá de la vida cotidiana de las personas: se encuentra en el diario vivir; con estos *spyware* las empresas intentan recolectar información para comercializar sus productos y obtener información de las personas sin pagar por ella y sin su consentimiento.

Ingeniería social (seguridad informática)

"En el campo de la seguridad informática, *ingeniería social* es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Es una técnica que pueden usar ciertas personas, tales como investigadores privados, criminales, o delincuentes computacionales, para obtener información, acceso o privilegios en sistemas de información que les

permitan realizar algún acto que perjudique o exponga la persona u organismo comprometido a riesgo o abusos"[6].

Las personas no poseen privacidad y, con tal de obtener sus cuotas de mercado, las empresas están dispuestas a violar la privacidad de sus mismos consumidores. En opinión del autor de este trabajo, este es un método muy común e incluso necesario para ser competitivo en el mercado, así las empresas les dan vigencia a estas prácticas, bien sea por ser competitivas en el mercado o por crear mejores productos para sus clientes, lo cual no representa un verdadero problema en cuanto exista respeto y confidencialidad con esta información que las empresas están obteniendo de sus clientes.

¿Pero, cómo funciona?

"El principio que sustenta la ingeniería social es el que en cualquier sistema "los usuarios son el eslabón débil". En la práctica, un ingeniero social usará comúnmente el teléfono o Internet para engañar a la gente, fingiendo ser, por ejemplo, un empleado de algún banco o alguna otra empresa, un compañero de trabajo, un técnico o un cliente. Vía Internet o la web se usa, adicionalmente, el envío de solicitudes de renovación de permisos de acceso a páginas web o memos falsos que solicitan respuestas e incluso las famosas "cadenas", llevando así a revelar información sensible, o a violar las políticas de seguridad típicas. Con este método, los ingenieros sociales aprovechan la tendencia natural de la gente a reaccionar de manera predecible en ciertas situaciones, –por ejemplo proporcionando detalles financieros a un aparente funcionario de un banco– en lugar de tener que encontrar agujeros de seguridad en los sistemas informáticos"[7].

El eslabón más débil de la cadena

"Allen H Beiner, consultor en sabotaje electrónico del FBI, afirma que el enlace más débil con respecto a la protección de datos comerciales vitales es el trabajador mismo. 'Podemos colocar *firewalls* (cortafuegos) en cada una de las computadoras pero en realidad todo depende de la persona', agrega el consultor. Según datos de un cálculo estimativo, dos tercios del total del espionaje corporativo en los EE.UU. es desarrollado por los propios empleados. En algunas ocasiones, los empleados venden secretos corporativos con fines de lucro. En otros casos, pueden hacerlo por venganza. Un empleado disconforme es capaz de enviar sus secretos corporativos directo a la competencia" (Blogg, Op. cit.)

Se debe cuidar incluso a los empleados de la empresa que tienen acceso a los activos intangibles de la empresa, por lo cual es importante que la rotación de personal dentro de las empresas no sea muy alta, sino que constituye una buena medida para cuidar la información de la empresa.

6 Ingeniería social (seguridad informática) [en línea] Wikipedia. 12 de febrero de 2011 [consultado: 1 de mayo de 2011] Disponible en: [http://es.wikipedia.org/wiki/Ingenier%C3%ADa_social_(seguridad_informática)].

7 Op. cit. Ingeniería social (seguridad informática).

A lo anterior el autor de este trabajo pretende dar solución por medio de mejores prácticas empresariales en el sentido que los ambientes de trabajo. Las recompensas y distintas motivaciones que la empresa debe ofrecer a su recurso humano deben estar encaminadas a que este esté satisfecho con su trabajo y por ende exista una colaboración más amena entre la empresa como organización y sus empleados. La empresa debe entrar a trabajar por el puesto de trabajo, no solo el puesto de trabajo debe trabajar para la empresa.

Desarrollo de una política de seguridad para la empresa

Tabla 1. **Principales factores para medir el nivel de seguridad de la empresa (seguridad informática) (Chapin y Akridge, 2005).**

Métrica	Supuesta medición	Peligros
Número de virus o códigos malignos defectados	Eficacia de los controles antivirus automáticos	¿Por qué pasan tantos virus en primer lugar? ¿Cuántos pasaron y nunca se detectaron?
Número de incidentes e investigaciones de seguridad	Nivel de actividad de la monitorización de eventos de seguridad	¿Qué umbral desencadena un incidente o una investigación? ¿Se desencadenan incidentes por defectos en los procedimientos organizativos?
Coste de las brechas de seguridad	Pérdidas económicas reales debidas a fallos de seguridad	¿Qué riesgos residuales eligió asumir la empresa? ¿Es una medida de la respuesta ante crisis o desastres, pero no necesariamente función de las salvaguardas sensatas implantadas?
Recursos asignados a las funciones de seguridad	Coste económico real de utilizar un programa de seguridad	¿Son ineficientes las herrameintas, tareas asignadas o procedimientos, llevando al personal a perder tiempo?
Cumplimiento de las reglas de seguridad	Nivel de cumplimiento de los objetivos del programa de seguridad	¿Cómo se relaciona el cumplimiento con la eficacia? ¿Cuál es el orden de cumplimiento? Una vez logrado el cumplimiento. ¿Se "acaba" el programa de seguridad?

Una empresa en la que sea crucial el correcto dominio de la información y la absoluta confidencialidad, debe tener en cuenta estos factores para proteger sus activos intangibles y así garantizar su mejor uso.

Vulnerabilidad de la información electrónica

"La información más valiosa actualmente está almacenada de forma electrónica y, dado que las computadoras están conectadas a redes y en línea, o accesibles por otros medios físicos, el director de sistemas juega un papel fundamental en la defensa de la corporación frente a las actividades de espionaje (y en la detención de esas actividades cuando se descubren). A pesar de que lo más probable es que los incidentes de espionaje corporativo no puedan erradicarse completamente, las corporaciones pueden modificar sus estrategias de seguridad para reducir al mínimo los incidentes y las pérdidas que provocan" (Guillermo, 2003).

La actual incursión de las nuevas tecnologías de forma cada vez más acelerada ha causado que los datos sean más vulnerables, debido a que estos se encuentran en un medio de acceso global

para el cual no se necesita de los documentos físicos para obtenerlos. Con ello la conectividad ha aumentado pero esta se debe restringir por medio de la formulación de políticas restrictivas hacia la información más vulnerable.

De esta información recolectada podemos evidenciar que las tendencias están encaminadas a no respetar el juego limpio entre organizaciones de un mismo sector, en donde las organizaciones suponen que deben colaborar, compiten de forma agresiva robándose las ideas de sus competidores directos, hurtando información e ideas. Esto tiene una justificación desde una visión financiera, ya que muchas empresas lo hacen para ahorro de costos y una justificación desde la estrategia empresarial, realizando estos robos para apropiarse de una ventaja competitiva y convertirla en propia o tan solo para frenar esta ventaja en los competidores y que estos no tomen mayores partidas de mercado. Pero estas justificaciones están basadas en actos inmorales de hurto realizadas por organizaciones prestigiosas en las cuales sus consumidores depositan la información, por lo cual muchos de estos casos de hurto quedan en el olvido y no se les hace mucha propaganda, para no perder porciones de mercado importantes por desprestigio.

Conclusión

El espionaje corporativo afecta directamente a las organizaciones; al ser la estrategia una vista de los objetivos de la empresa a largo plazo lo hace uno de los principales factores afectados por el espionaje corporativo, y así no se puede ver como un problema a corto plazo, puesto que afecta a los proyectos a largo plazo de la empresa. Todo comienza con la simple fuga de información de un proyecto de la empresa, luego las empresas competidoras pueden tomar partida de ello para cambiar su portafolio, imitar el de los competidores o adelantarse a los movimientos de ese competidor que perdió esa valiosa información. Esto lleva a una anulación inmediata de toda estrategia en torno a la información fugada, puesto que los competidores van a estar más adelante. Así, si la ventaja competitiva es uno de los principales objetivos de la estrategia. Esta ventaja nunca se logrará, se perderán millones por estudios y por esa ventaja que se perdió, además de costos asociados a la recuperación de la compañía para seguir siendo competitiva en el mercado. Todo lo anterior es un análisis desde la estrategia empresarial.

Por esto, el mercado se ve directamente afectado, se convertirá en un mercado depredador en el que las compañías de un mismo sector industrial no colaboran entre sí para salir adelante y buscar la mejor forma de satisfacer a los consumidores, que se supone que son el objetivo de la oferta en el mercado. Cabe hacer salvedad en que este objetivo está directamente relacionado con la obtención de rentabilidad de los empresarios, pues entre más satisfecho el cliente lo más probable es que se obtengan mayores rentabilidades. Retomando, las compañías se vuelven depredadoras de otras compañías buscando establecerse como monopolios en el mercado. ¿Cuál es el problema de los monopolios? Pues que el consumidor se relega a aceptar productos idénticos, el mercado pierde diversidad y ya no hay de donde escoger más que de un solo productor; esto nos lleva a otro problema en el mercado: se pierde la competencia, por lo cual se pierde esa referencia oponente que hace que las empresas de un sector luchen entre sí de cierta manera apoyándose para mejorar a partir de la lógica de intentar estar en primer lugar.

Lo dicho en el anterior párrafo muestra como el mercado se ve afectado por la pérdida de información de una empresa, convierte al mercado en uno supremamente desigual e injusto, donde el que más pueda obtener información es el ganador, puesto que la oportuna información es poder en el mercado. Dicho esto, los consumidores pueden beneficiarse en cuanto a precios, puesto que una competencia caníbal por conseguir mayores partes de mercado entre empresas probablemente reduzca los precios y los consumidores pueden obtener productos mucho más baratos con mejores características, lo cual se parece mucho a la piratería. Esta competencia caníbal también puede hacer subir los precios a los productos legítimos, siendo así más costoso producirlos para las marcas legítimas. Aquí lo importante no es la reducción de costes sino que se perderá la motivación que tienen las empresas para innovar y producir desarrollo, puesto que todo lo que hacen será copiado, mejorado, robado, no se podrá incentivar para que las empresas sigan mejorando sus productos, así estas copias a precios más bajos serán solo una ventaja a corto plazo, pero a largo plazo, será una gran desventaja para la estrategia de la empresa, el mercado y en últimas el consumidor.

Otro punto importante a tratar es que el eslabón más débil de una compañía a la hora de proteger su información, son los mismos empleados, porque se pueden tener los mejores *software* para impedir intrusos, se puede tener seguridad, muros muy altos y claves indescifrables, pero esta información que se intenta proteger siempre está disponible para un grupo de personas que trabajan dentro de la organización. Estas personas, al tener conocimiento de esta, la pueden distribuir, y aquí es donde entra la importancia de mantener dentro de las empresas una rotación baja o nula de personal clave para las operaciones de la misma, manteniendo ambientes de trabajo sanos y motivadores: así se podría solucionar gran parte del problema.

Aun así se deben implementar mejoras en las leyes de seguridad, principalmente en seguridad informática, puesto que en la actualidad el desarrollo de las tecnologías ha causado que todos los archivos e información estén en forma electrónica y no en físico, lo cual los hace mucho más vulnerables. Se debe poner mucha más atención a estos casos de robo de datos, siempre es difícil juzgarlos puesto que es difícil poner la línea entre la ilegalidad de tomar archivos propiedad de otros y los archivos que son disponibles para todos y no representa un delito saberlos o usarlos para beneficio propio.

El panorama es complejo, un problema que requiere de tiempo más aun en un país como Colombia, en vía de desarrollo, al cual le falta mucho por descubrir e implementar, por lo cual debemos no solo seguir los pasos de países más desarrollados sino crear nuestros propios modelos de seguridad, para que se garantice la privacidad de la información, lo cual le dará legitimidad y mayor valor a los productos del mercado, influyendo en que los clientes estén más satisfechos y a su vez generando una dinámica de mercado apropiada donde las empresas se dinamicen.

Referencias

Blogg, Keith. *Espionaje Corporativo* [en línea] Foro de Seguridad: Foro de Profesionales Latinoamericanos de Seguridad. Disponible en: [http://forodeseguridad.com/artic/segcorp/7208.htm]. Consultado el 1 de mayo de 2011.

Chapin, David A. y Steven Akridge (2005). ¿Cómo Puede Medirse la Seguridad? [En línea] Information Systems Control Journal, Volumen 2. Disponible en: [http://www.iso27000.es/download/HowCanSecurityBeMeasured-SP.pdf]. Consultado el 1 de mayo de 2011.

Ley Sarbanes-Oxley [en línea] Wikipedia. Disponible en: [http://es.wikipedia.org/wiki/Ley_Sarbanes-Oxley]. Consultado el 9 de marzo de 2011.

Guillermo R., Edwin E. (2003). *Espionaje corporativo: "un mal que aqueja a miles de empresas"* [en línea]. Gestiopolis. Disponible en: [http://www.gestiopolis.com/canales/gerencial/articulos/69/espicorporativo.htm]. Consultado el 21 de febrero de 2011.

Guillermo R., Edwin E. *Espionaje corporativo* (2003). [En línea]. Monografías. oct. 2003. [consultado 21 feb. 2011]. Disponible en: [http://www.gestiopolis.com/canales/gerencial/articulos/69/espicorporativo.htm]. Consultado el 21 de febrero de 2011.

Trends in Proprietary Information (1999). Loss - Tendencias en la pérdida de información confidencial, American Society for Industrial Security and PricewaterhouseCoopers.

Ingeniería social (seguridad informática) (2011). [en línea] Wikipedia. Disponible en: [http://es.wikipedia.org/wiki/Ingenier%C3%ADa_social_(seguridad_informática)]. Consultado el 12 de febrero de 2011.