APUNTES SOBRE LA INVERSIÓN Y GESTIÓN DE LA SEGURIDAD INFORMÁTICA - Junio 2004

Link- http://www.virusprot.com/Art49.html

Introducción

Observando los resultados de la encuesta internacional de *Information Security Magazine* de Abril de 2004 (Briney 2004), las inversiones en seguridad informática muestran una constante: fortalecimiento del perímetro de seguridad, actualización de infraestructura de seguridad y administración de la seguridad informática. Mucha de esta inversión se concentra en aspectos de hardware, software y servicios, lo cual sugiere un concepto de seguridad informática orientado por el modelo de riesgos y controles, que si bien aporta elementos importantes para el mantenimiento de niveles de seguridad informática adecuados para la realidad de cada organización, limita la comprensión de eventos inesperados que generalmente no encuentran respuesta a los mismos y cuestionan el modelo de seguridad informática de la empresa.

En este sentido, el reto de la inversión en seguridad informática y el valor agregado que esta produce para las actividades del negocio establece una serie de interrogantes y cuestionamientos que los encargados de la misma deben responder a la alta gerencia. Esta respuesta debe estar en términos de la gestión de la seguridad informática de la organización y las implicaciones económicas que trae el mantenimiento de esta función.

Caracterizando la Inversión en Seguridad Informática

De acuerdo con Anderson (2001) existen tres características fundamentales asociadas con el mercado de tecnologías de información (TI):

- El valor de un producto para un usuario depende de cuántos exitosamente lo han adoptado.
- La tecnología tiene altos costos fijos y bajos costos marginales.
- Existen frecuentemente altos costos para los usuarios con el cambio de tecnologías.

Dichas características establecen una competencia de los proveedores por conquistar segmentos de mercado importantes, sabiendo que el ganador se lleva todo. Pero la pregunta es: ¿Quién es el beneficiado de esta dinámica? ¿La empresa? ¿El mercado de productos?

La seguridad informática, no es ajena a estas características propias del mercado de TI, pues, como comentamos previamente, el hardware, el software y los servicios especializados, son parte de la dinámica de la función de seguridad informática en las organizaciones.

La inversión en seguridad informática es un reto para los encargados de este tema en las organizaciones. Surgen preguntas alrededor del tema de presupuesto, impacto y retorno de la inversión que en la actualidad causan revuelo y establecen muchos interrogantes para aquellos que se hayan en la tarea de justificar presupuestos de seguridad informática.

Consideremos algunas ideas para tratar de aproximarnos a esta difícil tarea de los que tienen a cargo el área de seguridad. Dado que generalmente las inversiones en seguridad informática

se justifican en función de los riesgos y niveles de riesgo a los que puede o podría estar expuesto una organización, podríamos sugerir una adaptación de la matriz de tipos de inversión presentada en Remenyi, D., Money, A., Sherwood-Smith, M. y Irani, Z (2000):

RIESGO/VISIBILIDAD	Alto	Proyecto Estratégico	Proyecto de Actualización
	Bajo	Proyecto de Negocio	Proyecto Cotidiano
		Alto	Bajo
	IMPACTO/GANANCIA		

Tabla No.1 Matriz de tipos de inversión en seguridad informática. (Adaptado de Remenyi, D., Money, A., Sherwood-Smith, M. y Irani, Z. 2000. pág. 43)

La matriz sugiere como elementos de análisis dos componentes: *riesgo/visibilidad* e *impacto/ganancia*. El primero entendido de la manera tradicional establecida en el modelo de riesgos y controles donde la inversión se concentrará en atender las zonas valoradas como de mayor riesgo con el fin de mitigar los mismos a través de medidas de control que permitan atenderlos adecuadamente. En esta medida, al atender estos riesgos se aumenta la visibilidad del área de seguridad, por su diligencia y debido cuidado en el mantenimiento de bajos niveles de riesgo asociados con la arquitectura de cómputo que apoyan las funciones de negocio. El segundo expone la importancia desde el punto de vista del negocio y las ganancias (tangibles e intangibles) que se puedan derivar del proyecto mismo. Es la zona donde los gerentes confirman y entienden en términos de estrategias de negocio cómo el proyecto hace parte de la cadena de valor que se plantea para el producto o servicio en el cliente.

Si bien esta propuesta inicial de análisis de tipos de inversión orientada por proyectos, no pretende solucionar la problemática de la inversión en seguridad informática, busca sugerir una ruta complementaria entre la función de seguridad y la estrategia de negocio que trate de coordinar los esfuerzos e intereses de las partes para que el beneficiario final, el cliente, sea quien tenga el mayor valor y confianza en el uso de los productos o servicios que provee la organización.

Con esta breve explicación revisemos los diferentes cuadrantes y alternativas en el contexto de los proyectos de seguridad informática.

Proyecto Estratégico

Este cuadrante define un proyecto donde el área de seguridad informática, frente a su evaluación de riesgos y controles y la gerencia de la organización frente a su función de negocios, comprenden e integran sus perspectivas buscando el mayor impacto corporativo y de negocio, articulando una solución de seguridad informática robusta y confiable que aumenta la confianza del cliente y sugiere un mayor uso de los servicios de la empresa. El factor clave en este punto desde la óptica del cliente y la organización es confianza, y desde la visión del área de seguridad es seguridad funcional y operativa y, menor exposición a los riesgos.

Proyecto de Actualización

Una iniciativa de este estilo donde los riesgos asociados son altos, dado los cambios sensibles que suscitan una actualización, particularmente en el área de seguridad, frente a un bajo impacto en la operación de la organización en sus labores de negocio, establecen una ruta crítica de valoración del riesgo de negocio por parte del área de seguridad, que le permitan adecuar sus funciones para soportar la confianza de la operación de negocios sin traumatismos. El factor clave en este punto para el área de seguridad es coordinación y

adaptación, y desde la perspectiva del cliente y la organización es efectividad y continuidad de la operación.

Proyecto de Negocio

Un proyecto de este estilo esta marcado por la influencia fuerte de un comportamiento de mercados, un alto impacto frente a la competencia y mucho valor agregado para el cliente. La seguridad informática en este tipo de iniciativas debe balancear las implicaciones de seguridad de lo servicios o productos propuestos, pues de no hacerlo será mirado como el "entorpecedor" de proyectos. Debe existir un acuerdo o "*trade-off*" de partes donde se establecen que se puede esperar de la seguridad y que esta dispuesta a ceder dentro de los parámetros mínimos requeridos, así como lo que esta dispuesto a aceptar y ceder la función de negocio frente al tema de seguridad. El factor clave en esta distinción para el área de seguridad es negociación y agilidad y desde el punto de vista del cliente y la organización confianza y valor agregado.

Proyecto Cotidiano

Finalmente este tipo de proyectos o inversiones de seguridad en este cuadrante, son aquellas que generalmente son de orden interno y administrativo que le permiten a la organización avanzar en el fortalecimiento de su características de seguridad informática. Los proyecto cotidianos deben comprometer a la gerencia con la seguridad de información como prerrequisito para aumentar sus niveles de frente a los proceso de negocio. El factor clave en este cuadrante para el área de seguridad es concientización y regulación y para el cliente y la organización imagen y compromiso institucional.

Consideraciones sobre la Rentabilidad de la Inversión en Seguridad Informática

---

Si bien un aspecto crítico en el desarrollo de la función de seguridad informática es la inversión, la gestión y evaluación de dicha inversión es el complemento necesario para establecer los niveles de satisfacción y rentabilidad del cliente y la organización respectivamente.

Existen múltiples aproximaciones a la evaluación de los aspectos económicos de la seguridad informática (Gordon y Richardson 2004, Gordon y Loeb 2001), los cuales buscan establecer métricas y estimaciones de valor a través tanto de métodos cuantitativos como cualitativos. Dichos métodos sugieren aproximaciones que utilizan conceptos como el valor presente neto (VPN), retorno de la inversión (ROI), como los más sobresalientes, que tratan de explicar en términos numéricos la valoración de la seguridad informática para conceptuar sobre los beneficios y costos de la misma (generalmente tangibles) que permitan ofrecer herramientas a los encargados de la seguridad para hablar en los términos de la gerencia: inversión.

El VPN (Gordon y Loeb 2001, pág. 5-7) aplicado en la inversión en seguridad informática trata de maximizar las ganancias o minimizar las pérdidas, relacionadas con una planeación óptima de recursos (en términos de los diferentes temas de seguridad informática) para la operación de la función de seguridad y el cumplimiento de sus objetivos. En este sentido el VPN, considera los riesgos para valorar los beneficios y costos de la inversión en seguridad para aceptar o rechazar un aumento de la inversión en este tema.

Los razonamientos claves asociados con el VPN para seguridad informática son: (Gordon y Richardson 2004)

- *Entre más se dilate la implementación de la seguridad informática, menos se justificará la inversión*

Esta reflexión nos contextualiza en el escenario de los riesgos, es decir, mientras no se materialice el riesgo de seguridad informática será más complicado justificar una inversión. Una afirmación que se sustenta en un enfoque reactivo.

- *Entre más pronto haga la implementación de la seguridad informática, más costosa será la inversión*

Esta parte del razonamiento nos confronta frente al cambio tecnológico y altos costos fijos de operación y bajos costos marginales de uso, como previamente se comentaba en la sección caracterizando la inversión en seguridad informática. Un razonamiento basado en un enfoque de operación.

Luego se plantea una encrucijada para aquellos que requieran la evaluación del inversión en seguridad informática siguiendo el VPN, la cual es, no poder establecer el nivel óptimo de la inversión a menos que se materialice un evento adverso de seguridad que impacte la operación y materialice un riesgo valorado y establecido previamente.

Si bien el VPN ofrece elementos formales para estimar y justificar la inversión en seguridad, la alta dinámica de los cambios en seguridad y constante descubrimiento de fallas, hace que las estrategias de valoración y efectividad del presupuesto de seguridad informática sean poco confiables y generalmente intuitivas.

De otra parte el ROI, en contraste con el VPN, es una estrategia de medición para cortos períodos de tiempo (generalmente anual). El ROI es una ecuación que establece la efectividad de la inversión en un área determinada. Dicha ecuación considera el beneficio anual obtenido dividido el monto de la inversión efectuada. En este sentido, calcular el ROI para la inversión en seguridad informática, en una posición eminentemente técnica, sería establecer el total de la inversión en software y hardware, incluyendo los costos de instalación., actualización y entrenamiento requerido, en contraste con la cuantificación de los beneficios de la misma, lo cual podría sugerir ideas sobre menores incidentes de seguridad, bloqueos de ataques y menores tiempos de respuesta ante situaciones críticas, que se revisarían en términos de ahorros de dinero, si se hubiesen materializado.

En una perspectiva amplia de la seguridad informática, no sería viable calcular el ROI de la inversión de seguridad, dado que la seguridad informática es un asunto corporativo y no eminentemente tecnológico, lo cual requeriría entradas de muchas áreas de la organización, incluida el área de finanzas (Greengard 2003)

En este sentido, el ROI en la inversión en seguridad informática debe responder a un enfoque más sistémico de la organización particularmente orientado a la dualidad de la seguridad informática como lo es la inseguridad informática (Cano 2004). La idea inicial sugerida es cuantificar en términos de dinero el costo que tendría un incidente de seguridad informática específico, por ejemplo virus informáticos, frente a la inversión efectuada en temas de antivirus, con el fin de ilustrar el ahorro que hace la organización frente a la inversión en la plataforma antivirus de presentarse un incidente de este estilo.

Si bien es un caso básico para ilustrar la manera de hacerlo, extrapolarlo a otros elementos de seguridad informática requiere mayor análisis y reflexiones particulares a cada una de las infraestructuras de seguridad en las organizaciones.

Como hemos visto hasta el momento establecer la rentabilidad de la inversión en seguridad es un constante reto para comprender sus beneficios tangibles e intangibles, que buscan no solamente mantener niveles de aseguramiento y control del perímetro de seguridad de la organización, sino incorporar cada vez más la distinción de seguridad informática en la esencia misma de los negocios de la organización, un permanente acuerdo o "*trade-off*" para mantener la coordinación entre la tecnología, los procesos y las personas.

Reflexiones Sobre la Gestión de la Seguridad Informática

Precisamente mantener la coordinación entre la tecnología, los procesos y las personas requiere establecer un marco de gestión integral que sintetice y aterrice las inversiones de seguridad informática para generar el valor esperado de la seguridad en el hacer mismo de la organización.

En el ámbito de la gestión de seguridad informática los modelos del NIST (2003), el BS-7799 o ISO 17799 (Cano 2001) son referentes interesantes que no establecen "cómos" operacionales sino lineamientos generales de acción que deben ser afinados y contextualizados en la realidad de cada organización. Sin embargo en el modelo del NIST, detallado en el documento "*Security Metrics Guide for Information Technology Systems*", se desarrolla el concepto de métrica de seguridad basado en la manera como se ejecutan y alcanzan objetivos y metas de seguridad informática, lo cual se materializa en los resultados deseados de la implementación de los programas de implementación requeridos para tal fin.

Esta dinámica sugerida por el modelo del NIST, esta soportada por un programa de métricas de cuatro componentes interdependientes: Soporte de la gerencia, políticas y prácticas, métricas cuantificables de ejecución y logro y, análisis de métricas. Cada uno de ellos establece una serie de requisitos y procedimientos de análisis que para contar con un reporte de la gestión de la seguridad como insumo para la toma de decisiones sobre el tema, así como las responsabilidades de los niveles y cargos de las personas que intervienen.

El modelo es exigente (dado el alto grado de detalle, datos y operatividad que requiere para su aplicación) y con una alta dosis de cuestionarios requeridos para detallar cada una de las áreas de evaluación que son objeto de esta guía. Sería temerario pensar que la guía fuese la solución al complejo conjunto de relaciones que sugiere la gestión de seguridad, unida al detalle de la inversión, pero si sugiere un camino formal para construir un puente entre la incertidumbre que propone la administración de la seguridad y el debido reporte y rendición de cuentas de los recursos que se le entregan a la función de seguridad.

Consideraciones Finales

La inversión y la gestión de la seguridad son dos temas complementarios, los cuales sugieren una capacidad sistémica y sistemática para comprender por una parte, las relaciones que exige la seguridad en una organización y por otro, la detallada y delicada lista de actividades y acciones que son requeridas para operacionalizar el concepto intagible de la seguridad informática.

Si bien la gestión de la seguridad informática es un fenómeno que poco se ha estudiado existen investigaciones y análisis del mismo que orientan y dan sentido a muchas de las actividades que intuitivamente se adelantan en las organizaciones para tratar de dar respuesta a la alta gerencia sobre este tema: ¿mi seguridad hoy es mejor que hace un año?.

Por tanto, las razones financieras y conceptos de evaluación de inversiones como el VPN y ROI, son estrategias interesantes para considerar evaluaciones y análisis puntuales de la inversión en seguridad informática, los cuales no pueden ser rápidamente extrapolables a niveles corporativos por la incidencia de factores y variables difícilmente cuantificables como los relaciones políticas, cambios de directivas, fusiones, entre otras. Sin embargo, aportan orientaciones económicas que deben ser revisadas en conjunto con el área financiera para lograr un lenguaje común que permita a la función de seguridad hablar el idioma de las finanzas y a las finanzas el dialecto de la seguridad.

En este sentido formalizar un modelo de gestión de seguridad que considere las áreas de finanzas, mercadeo, junta directiva, en pocas palabras las áreas de la operación y control del negocio, como fuentes mismas de los insumos del área de seguridad y un área de seguridad concebida desde y para el negocio, podría articular y dar sentido a las métricas cuantitativas (como ROI y VPN) y desarrollar en conjunto el concepto de valor agregado para el cliente

basado en alto niveles tecnológicos de seguridad, confianza en la operaciones y estrategia personalizada de negocios.

Finalmente hablar sobre gestión e inversión en seguridad es comprender que la seguridad informática no es mas que un permanente ciclo de tecnología, procesos y personas que establecen relaciones tangibles, en la asignación de recursos, para producir un bien intangible como lo es la seguridad informática.

Referencias

Gordon, L. y Richarson, R. (2004) The new economics of information security. *Securitypipeline Magazine*. March. <http://www.securitypipeline.com/showArticle.jhtml?articleID=18600228>

Gordon, L. y Loeb, M. (2001) Economic aspect of information security. *Rainbow Technologies*. http://www.rainbow.com/ library/8/EconomicsAspectsOfInformationSecurity.pdf

Anderson, R. (2001) Why information security is hard. An Economic Perspective. *Annual Computer Security Application Conference Proceedings*. <http://www.acsac.org/2001/papers/110.pdf>

Remenyi, D., Money, A., Sherwood-Smith, M. y Irani, Z. (2000) The effective measurement and management of IT Cost and benefits. Second Edition. Butterwoth Heinemann.

NIST (2003) Security Metrics Guide for Information Technology Systems - SP 800-55

<http://csrc.nist.gov/publications/nistpubs/800-55/sp800-55.pdf>

Briney, A. (2004) Doom or Boom? Fearing the worst, companies are diversifying their spending. *Information Security Magazine*. May. <http://infosecuritymag.techtarget.com/ss/0,295796,sid6_iss366_art687,00.html>

Greengard, S. (2003) The real cost of cybersecurity. *Business Finance Magazine*. April. <http://www.businessfinancemag.com/>

Cano, J. (2001) Reflexiones sobre estándares de seguridad informática. *Computer World Colombia*. Noviembre 15 - Noviembre 29.

Cano, J. (2004) Inseguridad informática. Un concepto dual en seguridad informática. *Computer World Colombia*. Marzo. (Disponible en: <http://www.virusprot.com/Art47.html>)

Sitios Web:
Economics of IT Security - <http://www.utdallas.edu/~huseyin/security.html>

D. Jeimy J. Cano
jcano@uniandes.edu.co
Ingeniero de Sistemas y Computación
Universidad de los Andes
COLOMBIA

El Doctor Cano es profesor de la Universidad de los Andes en la Facultad de Derecho y el Departamento de Sistemas y Computación, donde imparte cátedras relacionadas con delitos informáticos y computación forense. Es miembro investigador de la Red Iberoamericana de Criptología y Seguridad de la Información - CRIPTORED (http://www.criptored.upm.es) de la Universidad Politécnica de Madrid, moderador de la lista de seguridad informática de la ACIS - Asociación Colombiana de Ingenieros de Sistemas (http://www.acis.org.co) y conferencista nacional e internacional en temas relacionados con seguridad informática, delitos informáticos y computación forense.