Retorno de inversión de PCI DSS

Hacer una inversión de cualquier tipo requiere realizar un estudio previo que debe incluir el cálculo del retorno de dicha inversión (ROI). Si la inversión se refiere a seguridad de la información es habitual calcular el ROSI (*Return On Security Investment*). El cálculo de este valor se basa en dos conceptos: coste de la inversión y disminución del riesgo conseguida con dicha inversión. Bajo estas premisas, es factible demostrar que la implantación de la normativa PCI DSS es económicamente viable ya que la disminución del riesgo conseguida es mayor, en términos económicos, que el coste de la inversión realizada.

Javier Moreno Molinero

ROI vs ROSI

En el ámbito del control de gestión se conoce el retorno de inversión (en adelante, ROI) como la relación existente entre el coste de una inversión realizada y el beneficio obtenido. Se suele expresar como un porcentaje y se utiliza para calcular la viabilidad de un proyecto. Simplificándolo, un proyecto con ROI positivo será económicamente viable, ya que retornará al inversor más dinero que el que inicialmente invirtió. Por el contrario, un proyecto con ROI negativo será económicamente no viable, ya que no devolverá al inversor ni siquiera la cantidad que invirtió inicialmente. La fórmula básica para calcular el retorno de una inversión es:

ROI = (Beneficio - Coste)/Coste

En el ámbito de la seguridad de las tecnologías de la información existe un término, internacionalmente aceptado [1], para el cálculo del retorno de inversión de un proyecto de seguridad de la información: el ROSI (*Return On Security Investment*). Este concepto se utiliza para determinar la viabilidad de inversiones en seguridad que tienen por objetivo reducir el riesgo. La fórmula básica para calcular el ROSI es la siguiente:

ROSI = (Disminución de Riesgo - Coste) /Coste

En este caso, la disminución del riesgo asume el papel del beneficio debido a que la rentabilidad de una inversión en seguridad se espera que sea una disminución del riesgo al que está expuesta una organización, sistema o proceso. La disminución del riesgo se calcula conforme a la siguiente fórmula:

Disminución del Riesgo = Riesgo Expuesto x %Riesgo Mitigado

El riesgo expuesto viene determinado por la cantidad de ocurrencias –incidentes– de seguridad, así como por el impacto económico causado por cada incidente ocurrido. El riesgo expuesto se calcula, habitualmente, como una tasa anual:

Riesgo Expuesto = Coste de un incidente x Tasa de Ocurrencia Anual

ROSI en la adecuación a PCI DSS

Los fabricantes de tarjetas de pago (VISA, MasterCard, American Express, Diners y JCB) unificaron sus normativas de seguridad relativas a los datos de tarjetas de pago en la norma común PCI DSS *(Pay Card Industry Data Security Standard)*. Como es sabido, esta norma consta de doce requerimientos que debe cumplir toda entidad que trasmita, procese o almacene datos de tarjetas de pago. Multitud de empresas de todos los sectores (comercios, entidades financieras y proveedores de servicio) deben adaptar sus procesos y sistemas para cumplir con la norma PCI DSS.

¿Es esta adecuación un proyecto rentable? ¿Es medible económicamente la disminución del riesgo que supondrá la implantación de PCI DSS? ¿Se puede valorar económicamente el retorno de la inversión realizada para adaptar las organizaciones a la normativa PCI DSS?

Las cuestiones anteriores se resuelven calculando el ROSI de la implantación de la normativa PCI DSS. Para este cálculo es necesario obtener el valor de dos conceptos: Coste (del proceso de adecuación/ implantación) y Disminución del Riesgo (debida al alineamiento de la empresa con la norma PCI).

Se propone a continuación un ejemplo, que encajaría con una situación totalmente real consistente en un comercio de Nivel 1 que tiene más de seis millones de transacciones anuales, por ejemplo, de la marca VISA (estimando un total de ocho millones de transacciones al año de las cinco marcas de tarjetas promotoras de PCI DSS, es decir unas 22.000 transacciones al día). Esta empresa está estudiando la posibilidad de implantar la normativa PCI DSS y quiere comprobar si esta adecuación es económicamente rentable, para lo cual calcula el ROSI de dicha implantación. Se supone también que esta empresa sufre un solo incidente de seguridad relacionado con tarjetas de pago y que lo detecta con siete días de retraso. Suponiendo que únicamente el 75% de las tarjetas son comprometidas durante ese periodo de tiempo, el incidente de seguridad afecta a 115.500 tarjetas.

Cabe señalar que durante la elaboración de este artículo se produjo un incidente de seguridad [2], con gran repercusión pública, que avala la importancia de establecer fuertes medidas de seguridad para proteger los datos de tarjetas de pago.

Cálculo de la Disminución del Riesgo

Como se detallaba anteriormente, el cálculo de la disminución del riesgo se efectúa de la siguiente manera:

Disminución del Riesgo = Riesgo Expuesto x %Riesgo Mitigado
Riesgo Expuesto = Coste de un incidente x Tasa de Ocurrencia Anual

El coste de un incidente relacionado con tarjetas de pago es un dato difícil de obtener debido a que las empresas pocas veces recopilan un histórico de incidentes y menos aún publican estos datos (exceptuando aquellos países donde esta situación está legislada), dado el alto impacto que esto tendría en su imagen de marca.

Aun así, los pocos incidentes de los que se tiene información muestran que los factores fundamentales para calcular el coste de un incidente con tarjetas de crédito o débito son los siguientes:

1. Coste de multa de la entidad emisora de la tarjeta.
2. Coste de la investigación forense del incidente.
3. Coste de reemplazar las tarjetas.
4. Coste del fraude realizado.
5. Coste de sanciones relativas a LOPD.

Multas VISA en caso de incidente con tarjetas de pago en comercios					
Level	Initial Fee	Insufficient remediation	Monthly PCI DSS Violation After 4 months	Monthly PCI DSS Violation After 5 months	Monthly PCI DSS Subsequent months
Level 1	50.000 €	30.000 €	50.000 €	75.000 €	75.000 €
Level 2	25.000 €	15.000 €	25.000 €	50.000 €	50.000 €
Level 3	10.000 €	5.000 €	10.000 €	15.000 €	15.000 €
Level 4	10.000 €	5.000 €	10.000 €	15.000 €	15.000 €

Figura 1.- Multas VISA en caso de incidente con tarjetas de pago en comercios.

6. Coste de la pérdida de productividad de los empleados.
7. Coste de la restitución de imagen de marca.

A continuación se desgrana el cálculo de estos importes para el ejemplo propuesto:

1. Para el cálculo del coste de la multa por parte de los fabricantes de tarjetas al comercio se utiliza el programa de multas postcompromiso establecido por VISA [3]. Los escenarios que se establecen en este programa se detallan en la **figura 1**.

Así, si el comercio en el momento de producirse el incidente con tarjetas no hubiera arrancado ningún programa de adecuación a PCI DSS y teniendo en cuenta que los comercios de nivel 1 necesitan, según nos demuestra la experiencia, una media de un año para adecuar sus procesos a PCI DSS, la multa impuesta por VISA ascendería a 730.000 euros (50.000+30.000+ 50.000+75.000+[7x75.000]), siempre y cuando un año después el comercio pueda demostrar su cumplimiento.

2. La empresa que sufre un incidente de seguridad relacionado con tarjetas debe hacerse cargo de los costes de la Investigación Forense que exige VISA. En estas investigaciones forenses se debe presentar un informe preliminar a los tres días. Posteriormente, en función de la gravedad del incidente y del tamaño del comercio, la auditoría puede alargarse varios días o incluso semanas. Se supone un coste medio de 30.000 euros para estas investigaciones forenses.

3. Los fabricantes de tarjetas también pueden requerir al comercio que se haga cargo de los costes necesarios para reemplazar las tarjetas cuya información ha sido comprometida. Se estima que el coste medio de reemplazar una tarjeta es de dos euros [4].

4. Dependiendo de los resultados de las investigaciones forenses y de distintas clausulas existentes en contratos, los fabricantes pueden exigir a la entidad responsable del incidente de seguridad asumir el fraude realizado con las tarjetas comprometidas. Tanto el fraude total realizado como la proporción en que lo asumirán los distintos agentes implicados variarán dependiendo de multitud de variables como contratos y seguros existentes, responsabilidades penales exigibles, etc. Para el ejemplo propuesto, se supone un fraude de entre 5 y 20 euros por tarjeta y un seguro que protege al comercio de un fraude de hasta medio millón de euros.

5. Si el incidente de seguridad implica el compromiso de datos de carácter personal, existe la posibilidad de tener que hacer frente al pago de una sanción correspondiente a la vulneración de la Ley Orgánica de Protección de Datos. El importe de esta sanción puede oscilar entre 40.000 euros y 600.000 euros.

6. En el caso de que una empresa sufra un incidente relacionado con tarjetas de pago, la productividad de sus empleados se verá afectada en dos planos: algunos empleados no podrán realizar sus rutinas de trabajo debido a las investigaciones forenses o a las medidas de contención desplegadas, y además ciertos empleados deberán abandonar su tareas habituales para destinar todo su esfuerzo a solventar y paliar el incidente de seguridad. Las pérdidas debidas a la disminución de la productividad de los empleados se estiman entre dos y ocho euros [4] por tarjeta comprometida.

7. Por último, habría que incluir el coste correspondiente a la recuperación de la imagen de marca dañada después del incidente. La marca del comercio afectado se verá negativamente afectada por haber incurrido en un incidente con datos de tarjetas y la compañía se verá obligada a hacer un esfuerzo, fundamentalmente de marketing, para conseguir aminorar la fuga de clientes, así como para disminuir la dificultad a la hora de conseguir nuevos clientes. Se valora este esfuerzo económico entre medio millón y dos millones de euros.

En la **figura 2** se muestran, a modo de resumen, los costes asociados al incidente de seguridad descrito.

Teniendo en cuenta que únicamente se produce un incidente (tasa de ocurrencia anual) y que, como se indicaba anteriormente, la disminución del riesgo se calcula con las siguientes formulas:

Disminución del Riesgo = Riesgo Expuesto x %Riesgo Mitigado

COSTE DE UN INCIDENTE CON TARJETAS DE PAGO		
Tipo de Coste	Comercio Nivel 1 (Mínimo)	Comercio Nivel 1 (Máximo)
Multa	730.000 €	
Investigación Forense	30.000 €	
Reemplazar tarjetas	231.000 €	
Fraude realizado	577.500 €	2.310.000 €
Seguro Antifraude	-500.000 €	
Sanción LOPD	40.000 €	600.000 €
Pérdida productividad	231.000 €	924.000 €
Restitución Imagen de Marca	500.000 €	2.000.000 €
TOTAL	**1.839.500 €**	**6.325.000 €**

Figura 2.- Coste de un incidente con tarjetas de pago.

Riesgo Expuesto = Coste de un incidente x Tasa de Ocurrencia Anual

Y suponiendo que la implantación de PCI DSS mitiga al 90% el riesgo de que se produzcan incidentes de seguridad en datos de tarjetas de pago, se puede afirmar que la Disminución del Riesgo al implantar la normativa fluctúa entre 1.655.550 y 5.692.500 euros en el caso del comercio de nivel 1 propuesto como ejemplo.

Cálculo del coste de implantar PCI DSS

La implantación de la normativa PCI DSS en cualquier organización implica tres costes básicos:

- Coste de consultoría (análisis situación inicial o *gap analysis*, valoración de riesgos, diseño del plan de acción).
- Coste de adaptación de sistemas y procesos a PCI DSS (implantación del plan de acción que define las tareas para solventar los no cumplimientos).
- Coste de la auditoría de cumplimiento (auditoría *on site* anual que debe ser realizada por un QSA –*Qualified Security Assessor*–).

El cálculo de los costes de consultoría requiere un estudio minucioso de los procesos y sistemas incluidos en el entorno PCI de la entidad en cuestión. En el ejemplo expuesto, estos costes pueden oscilar entre 10.000 y 50.000 euros. El coste más elevado en el proceso de implantación de PCI DSS es, sin duda, el debido a la ejecución de las acciones correctivas de los no cumplimientos detectados en la etapa de consultoría. El importe de estos costes dependerá de la estrategia elegida, así como de la flexibilidad de las organizaciones para segmentar sus redes, eliminar datos de tarjetas de pago, externalizar servicios, etc. En el ejemplo planteado, estos costes pueden fluctuar entre medio millón de euros y dos millones de euros. Una vez implantadas todas las medidas correctoras y de cara a certificar el cumplimiento de la norma PCI DSS, las entidades deben someterse a una auditoría *on site* realizada por un QSA. El coste de esta auditoría puede oscilar entre 15.000 y 50.000 euros para un comercio de nivel 1.

Cálculo del retorno de inversión en la implantación de PCI DSS

Dado que el ROSI se calculaba mediante la siguiente fórmula:

ROSI = (Disminución de Riesgo - Coste) /Coste

Se puede afirmar que la implantación de PCI DSS tendrá, para el comercio propuesto como ejemplo, un retorno de inversión que oscilará entre un 171% y un 215%. Este caso parte de la premisa de que la inversión realizada se quiere recuperar en un solo año; el ROSI sería mucho mayor si se amortizaran los costes de la implantación durante un ciclo mayor (tres o cuatro años), aunque en ese supuesto habría que tener en cuenta el coste del mantenimiento de la certificación.

Conclusión

Como conclusión se puede afirmar que existe un método para calcular la viabilidad económica de realizar una inversión para adaptar las compañías a los requisitos de PCI DSS y que este método, en el ejemplo planteado, revela que el retorno de inversión de esta adecuación es positivo.

El supuesto mostrado debe ser entendido únicamente como un ejemplo que se apoya en los costes y situaciones específicamente propuestos. La implantación de la normativa PCI DSS y el retorno de la inversión correspondiente deben ser estudiados pormenorizadamente en cada caso concreto. ■

Javier Moreno Molinero
Account Manager
CISSP, GSEC
INTERNET SECURITY AUDITORS

[1] ISACA, http://www.isaca.org/Knowledge-Center/Standards/Documents/G41-ROSI-5Feb10.pdf.
[2] Sony Online Entertainment, http://www.soe.com/securityupdate/
[3] http://ask.barclaycard.co.uk/business/allfaqs/1_fraud_security/fines_2
[4] Forrester Research, *Calculating the cost of a security breach*, Ponemon Institute, *Fourth Annual US Cost of Data Breach Study* y Verizon, *2010 Payment Card Industry Compliance Report*.