ADMINISTRACION DE RIESGOS DE LA BANCA POR INTERNET
Por Ganesh Ramakrishnan

Los últimos años se han caracterizado por los rápidos cambios en la tecnología y por la introducción de servicios de banca corporativa y personal a través de Internet. La velocidad sin precedentes con la cual se están adoptando las nuevas tecnologías, la ubicuidad y naturaleza global de las redes electrónicas, la integración de plataformas de e-banking con los sistemas anteriores y la creciente dependencia de los bancos respecto de los terceros proveedores de servicios de información, tienden a amplificar dramáticamente la magnitud de los riesgos a los que están expuestos los bancos.

Muchos bancos han asumido que la banca por Internet aumenta principalmente los riesgos de seguridad de la información y no se han focalizado suficientemente sobre los efectos de otros riesgos específicos de la banca. Las disciplinas de administración de riesgos no han evolucionado a la misma velocidad y muchas instituciones, especialmente las de menor tamaño, no han podido incorporar controles de riesgos de banca por Internet dentro de las estructuras existentes de administración de riesgos. Este artículo provee un vistazo general sobre los distintos riesgos que se ven intensificados con la banca por Internet, y un enfoque holístico sobre la administración de los mismos.

Tipos de Banca de Internet

Las ofertas por Internet de las instituciones financieras pueden ser clasificadas en forma amplia en tres grandes grupos con distintos perfiles de riesgo:

- Informativas – Ofrecen información acerca de los productos y servicios del banco ("brochureware") y son de bajo riesgo.

- Comunicativas – Ofrecen información relacionada con las cuentas y posiblemente también actualizaciones de los datos estáticos (tales como domicilios) . Como se permite el acceso a los sistemas principales del banco, el riesgo es material.

- Transaccionales – Permiten a los clientes ejecutar transacciones financieras y acarrean el mayor riesgo. Algunos modelos transaccionales acarrean mayores riesgos, por ejemplo, si el cliente no ha visitado jamás una sucursal del banco durante toda su relación y prefiere llevar a cabo todas sus transacciones en forma remota (esto sucede comúnmente con algunos sitios de comercio de acciones en línea).

Riesgos de la Banca por Internet

La banca por Internet no abre nuevas categorías de riesgos, sino más bien acentúa los riesgos que enfrenta cualquier institución financiera. El directorio y la alta gerencia deben conocer estos riesgos y tratar con ellos en forma apropiada. Estos riesgos, que a veces se superponen, se pueden describir brevemente como sigue:

- Riesgo Estratégico – Este es el riesgo actual y prospectivo para las ganancias y el capital que surge de decisiones de negocio adversas o implementación inadecuada de decisiones de negocio. Muchos gerentes no comprenden plenamente los aspectos técnicos y estratégicos de la banca por Internet. Estimulados por las presiones de la competencia y de sus pares, los bancos pueden buscar introducir o expandir la banca por Internet sin realizar previamente un

adecuado análisis costo-beneficio. La estructura y recursos de la organización podrían no tener las habilidades para administrar la banca por Internet.

- Riesgo de Transacción – Este es el riesgo actual y prospectivo para las ganancias y el capital que surge del fraude, error, negligencia e inhabilidad para mantener niveles esperados de servicio. Puede existir un alto nivel de riesgo transaccional con los productos de banca por Internet , por la necesidad de contar con controles internos sofisticados y disponibilidad constante. La mayoría de las plataformas de banca de Internet están basadas en nuevas plataformas que utilizan complejas interfaces para vincularse con los sistemas anteriores, aumentando en consecuencia el riesgo de errores en las transacciones. Hay también necesidad de asegurar la integridad de los datos y el no repudio de las transacciones. Los terceros proveedores también aumentan los riesgos de las transacciones, ya que la organización no tiene un completo control sobre el tercero. De no haber un proceso y conexiones fluidas entre el banco y el tercero, hay un alto riesgo de errores en transacciones.
- Riesgo de Cumplimiento - Este es el riesgo para las ganancias y el capital que surge de violaciones de, o no conformidad con, leyes, regulaciones y estándares éticos. El riesgo de cumplimiento puede conducir a disminuir la reputación, pérdidas monetarias reales y reducción en las oportunidades de negocios. Los bancos necesitan comprender e interpretar cuidadosamente las leyes existentes en la medida que se apliquen a la banca de Internet y asegurar consistencia con los otros canales tales como la banca de sucursales. Este riesgo se amplifica cuando el cliente, el banco y la transacción están en más de un país. Se agregan a los riesgos las leyes, procedimientos impositivos y requerimientos informativos conflictivos entre distintas jurisdicciones. La necesidad de mantener la privacidad de los datos de los clientes y de buscar el consentimiento de los mismos antes de compartir sus datos contribuye al riesgo de cumplimiento. Los clientes están muy preocupados acerca de la privacidad de sus datos y los bancos necesitan ser vistos como guardianes confiables de tales datos. Finalmente, la necesidad de consumar las transacciones en forma inmediata (directamente con el procesamiento) puede conducir a que los bancos relajen los controles tradicionales, que intentan reducir el riesgo de cumplimiento.
- Riesgo de Reputación – Este es el riesgo actual y prospectivo para las ganancias y el capital que surge de la opinión pública negativa. La reputación de un banco puede verse dañada por servicios de banca de Internet que sean pobremente ejecutados (ej: disponibilidad limitada, software con problemas, respuesta pobre). Los clientes son menos indulgentes con cualquier problema y en consecuencia hay expectativas más rigurosas en relación al desempeño del canal de Internet. Los vínculos de hipertexto podrían vincular el sitio de un banco con otros sitios y podrían reflejar un endoso implícito de los otros sitios.
- Riesgo de Seguridad de la Información - Este es el riesgo para las ganancias y el capital que surge de procesos laxos de seguridad de la información, que exponen a la institución a ataques maliciosos internos o de hackers, virus, ataques de denegación de servicios, robo de información, destrucción de datos y fraudes. La velocidad de cambio de la tecnología y el hecho de que el canal de Internet es universalmente accesible hace a este riesgo especialmente crítico.
- Riesgo de Crédito - Este es el riesgo para las ganancias o el capital que surge de una falla del cliente para satisfacer sus obligaciones financieras. La banca de Internet permite a los clientes aplicar desde cualquier lugar del mundo. Los bancos encontrarán extremadamente dificultoso verificar la identidad del cliente, si intentan ofrecer crédito instantáneo a través de Internet. También es dificultoso verificar colaterales y perfeccionar acuerdos de seguridad. Finalmente, podrían haber cuestiones sobre a qué país (o estado) se aplica la transacción.
- Riesgo de Tasa de Interés – Este es el riesgo para las ganancias o el capital que surge de movimientos en las tasas de interés (ej: tasas de interés diferenciales entre activos y pasivos y cómo son éstos impactados por los cambios en las tasas de interés). La banca de Internet puede atraer préstamos y depósitos de un gran conjunto de clientes. También, dado que se facilita la comparación de tasas entre bancos, la presión sobre las tasas de interés es mayor, acentuando la necesidad de reaccionar rápidamente a los cambios de las mismas en el mercado.
- Riesgo de Liquidez - Este es el riesgo para las ganancias o el capital que surge de la incapacidad de un banco para satisfacer sus obligaciones. La banca de Internet puede

aumentar la volatilidad de los depósitos y de los activos, especialmente de clientes que mantienen sus cuentas sólo porque están obteniendo una tasa mejor. Estos clientes tienden a cortar su relación si obtienen una tasa ligeramente mejor en cualquier otro sitio.

- Riesgo de Precio – Este es el riesgo para las ganancias o el capital que surge de cambios en el valor de portafolios comercializados o instrumentos financieros. Los bancos pueden estar expuestos al riesgo de precio, si ellos crean o expanden la comercialización de depósitos, venta de préstamos o programas de securitización como resultado de las actividades de banca de Internet.
- Riesgo de Cambio de Moneda Extranjera – Esto surge cuando activos en una moneda están fundados en pasivos en otra. La banca de Internet puede alentar a los residentes de otros países a transar en sus monedas domésticas. Debido a la facilidad y al bajo costo de las transacciones, esto podría alentar a los clientes a tomar posiciones especulativas en distintas monedas. Grandes tenencias y transacciones en monedas no domésticas aumentan el riesgo de cambio.

Principios de Administración de Riesgos

Administrar los riesgos e implementar controles para las iniciativas de banca de Internet sigue los mismos principios que otros procesos de administración de riesgos. Lo más peligroso es tratar a esto como un problema técnico y dejarlo para que lo administre la gerencia de TI. Como lo ha mostrado la enumeración de riesgos anterior, este es un aspecto de administración general que requiere atención de la alta gerencia. Se expone abajo una estructura general de administración de riesgos:

Supervisión del Directorio y la Alta Gerencia

El directorio y la alta gerencia deberían establecer un efectivo control gerencial sobre los riesgos asociados con las actividades de e-banking, incluyendo responsabilidades específicas, políticas y controles para administrar estos riesgos. Además, la gerencia debería comprender claramente el rol de la banca de Internet en la consecución de los objetivos generales estratégicos de la institución. El negocio debería establecer objetivos específicos para la banca de Internet, tales como ingresos, ganancias, costos de transacciones y niveles de servicio. Un objetivo ambiguo establece el tono para una postura robusta de riesgo.

Los proyectos de banca de Internet pueden tener un impacto significativo sobre el perfil de riesgo de un banco y deberían ser revisados y aprobados por la alta gerencia. Esta debería llevar a cabo un análisis estratégico y de costo/recompensa apropiado. Además, la alta gerencia debería asegurarse que no se involucra en proyectos de e-banking a menos que tenga el conocimiento para la supervisión técnica y de administración de riesgos necesario a todos los niveles.

La alta gerencia debería poner el acento en la administración de riesgos estableciendo mecanismos claves de delegación y elaboración de informes , separación de tareas y procedimientos de escalamiento. La gerencia debería establecer un proceso formal de evaluación de riesgos en la organización, de forma tal que la gerencia de línea sea responsable por, y directamente involucrado en, identificación y mitigación de riesgos. Finalmente, la gerencia debería asegurar que se realizan análisis de debida diligencia (due diligence) y riesgo cuando el banco inicia o expande las actividades de banca de Internet.

Controles de Seguridad

Los controles de seguridad requieren atención especial por la naturaleza abierta de Internet y el devenir del cambio tecnológico.
Las áreas específicas de focalización incluyen:

- Autenticación – Esto significa asegurar que se verifican los clientes y se establecen sus identidades antes de realizar negocios sobre Internet. Las contraseñas (*passwords)*, los métodos biométricos, los sistemas de desafío-respuesta y la infraestructura de clave pública son algunas de las formas de fortalecer la autenticación. Hay una tendencia creciente hacia aplicaciones *"single-sign-on"* en las cuales el cliente necesita sólo una única ID para acceder a su entera relación con la entidad. Esto aumenta el riesgo de compromiso.
- No repudio – Los bancos deberían asegurarse que los clientes que transan en Internet no puedan denegar posteriormente haber originado las transacciones. Utilizando técnicas tales como PKI (certificados digitales), se puede lograr un fuerte no repudio. Sin embargo, en muchos países es aún dudosa su aplicabilidad.
- Segregación de tareas – Tal como en cualquier proceso tradicional, la segregación de tareas es vital para prevenir la perpetración de fraudes por cualquier individuo.

Los bancos deberían asegurar que hay medidas apropiadas para proteger la integridad de los datos de las transacciones de e-banking, de los registros y de la información. Todas las transacciones de e-banking deberían generar pistas claras de auditoría, las cuales deberían ser archivadas. Es también vital generar y proteger los registros de instrucciones de los clientes en un formato aceptable legalmente.

Los bancos deberían fortalecer los controles de seguridad de la información para preservar la confidencialidad e integridad de los datos de los clientes.
Algunos de los métodos disponibles son los *firewalls*, los tests éticos de hacking y los controles de acceso físico y lógico.

Administración de Riesgos Legales y de Reputación

La administración de riesgos legales y de reputación han sido divididos en:

- Privacidad – Los bancos deberían articular una política de privacidad y deberían comunicarla a sus clientes. A los clientes se les debería permitir optar por la divulgación y se debería ejercer un gran cuidado antes de compartir información de clientes con entidades externas. Si los clientes son de distintas jurisdicciones, se debe aplicar la ley de privacidad más estricta.
- Disponibilidad – Los bancos deberían contar con procesos de continuidad del negocio y planeamiento de contingencia para ayudar a asegurar la disponibilidad continua de los servicios de banca de Internet. Esto es desafiante por el alto volumen potencial de transacciones y por la demanda de disponibilidad de 24 horas al día y siete días por semana.
- Respuesta a Incidentes – Los bancos deberían formular planes apropiados de respuesta a incidentes para detectar, administrar, contener y minimizar los problemas que pudieran surgir de ataques internos y externos. Deberían haber pasos claros de escalamiento, una estrategia de comunicación a los clientes y la prensa y una cadena de comando documentada. Finalmente, debería haber un proceso para recolectar y preservar la evidencia forense luego de un evento adverso.

Los riesgos que surgen de la banca de Internet no están restringidos a las áreas de seguridad de la información, sino que se extienden a todas las áreas tradicionales de la banca. La administración de riesgos para la banca de Internet deberá ser dirigida por la alta gerencia e incorporada dentro de las disciplinas de administración de riesgos existentes en la organización. Los procedimientos de control necesitan alinearse con los rápidos cambios de la tecnología.