QUẢN TRỊ RỦI RO DỊCH VỤ NGÂN HÀNG TRỰC TUYẾN

Dương Kim Oanh*

Công nghệ không ngừng đổi mới, cuộc cạnh tranh gay gắt giữa các tổ chức Tài chính – Ngân hàng đang hoạt động cũng như các tổ chức Tài chính – Ngân hàng sắp bước chân vào thị trường buộc các ngân hàng phải mở rộng kênh phân phối của mình, đưa sản phẩm đến khách hàng sỉ và lẻ một cách nhanh chóng, tiện lợi thông qua kênh phân phối điện tử - được để cập đến như dịch vụ ngân hàng trực tuyến.

Dịch vụ ngân hàng trực tuyến giúp ngân hàng mở rộng thị trường, đa dạng hóa các loại hình sản phẩm và dịch vụ do tính năng dễ truy cập và linh hoạt của Internet. Nó còn có khả năng giúp ngân hàng gia tăng lợi nhuận vì chi phí thực hiện các giao dịch qua Internet thấp hơn nhiều so với chi phí giao dịch thông qua các kênh thông tin khác. Tuy nhiên, dịch vụ ngân hàng trực tuyến tiềm ẩn không ít rủi ro đối với hoạt động bảo mật, duy trì vị thế cạnh tranh của ngân hàng. Cụ thể là rủi ro chiến lược, rủi ro pháp lý và rủi ro uy tín của ngân hàng sẽ gia tăng.

Trong khuôn khổ bài viết này, tác giả xin nêu lên những rủi ro bắt nguồn từ đặc tính của dịch vụ ngân hàng trực tuyến và các quy định hiện hành (trên thế giới và tại Việt Nam) mà ngân hàng cần thiết áp dụng để quản trị rủi ro hiệu quả.

RỦI RO TRONG KINH DOANH DỊCH VỤ NGÂN HÀNG TRỰC TUYẾN

◆ Nguồn gốc rủi ro:

Bắt nguồn từ những đặc tính của dịch vụ trực tuyến, bao gồm:

- Tốc độ thay đổi nhanh chóng, khó dự báo của công nghệ và dịch vụ khách hàng: đòi hỏi về tính tiện lợi và nhanh chóng đối với dịch vụ của khách hàng ngày càng cao, đòi hỏi ngân hàng phải đón đầu những công nghệ mới để đáp ứng. Tuy nhiên, các biện pháp bảo mật, phòng ngừa rủi ro thường ra đời sau khi công nghệ đang sử dụng bị phát hiện có kẽ hở tiềm ẩn rủi ro. Ngoài ra, công nghệ hiện đại tiếp sau luôn là mối đe dọa đối với công nghệ trước.

- Đặc tính mở rộng toàn cầu của mạng lưới thông tin điện tử trực tuyến.

- Tính phụ thuộc ngày càng cao của ngân hàng vào chất lượng dịch vụ kỹ thuật do bên thứ ba cung cấp.

Mặc dù không tạo ra rủi ro mới, song những đặc tính trên đã góp phần đáng kể gia tăng các rủi ro truyền thống trong hoạt động của ngân hàng, đặc biệt phải kể đến rủi ro chiến lược, rủi ro pháp lý và rủi ro uy tín, từ đó ảnh hưởng đến danh mục rủi ro tổng thể của ngân hàng.

- Rủi ro chiến lược (*strategic risk*): Trước sự hấp dẫn của công nghệ mới và áp lực cạnh tranh, ngân hàng có thể quyết định xâm nhập vào một thị trường mới, hay cung cấp một sản phẩm trực tuyến mới mà thiếu sự nghiên cứu đầy đủ về công nghệ (những tiềm ẩn phía sau nó) và thiếu các nguồn lực cần thiết để khai thác thị trường, dẫn đến thua lỗ.

- Rủi ro pháp lý (*legal risk*): Xảy ra khi hệ thống giao dịch trực tuyến của ngân hàng không hoàn thiện, dẫn đến hai hậu quả: 1) không hỗ trợ tốt cho khách hàng: tài khoản của khách hàng bị hacker tấn công gây thiệt hại, nhầm lẫn trong cung cấp thông tin trực tuyến...2) không thể ngăn chặn rủi ro đạo đức từ phía khách hàng và ngân hàng bị thiệt hại.

- Rủi ro uy tín (*Reputational risk*): Là rủi ro vị thế và uy tín của ngân hàng bị đe dọa. Một

Đại học Ngân hàng Tp.HCM (*)

thông tin quan trọng trên trang chủ của ngân hàng bị thay đổi, thông tin về một trường hợp khách hàng bị thiệt hại do sử dụng dịch vụ trực tuyến của ngân hàng, dư luận xấu về công tác bảo mật của ngân hàng... đều gây khó khăn nghiêm trọng cho hoạt động của ngân hàng. ngân hàng sẽ khó có khả năng tiếp cận nguồn vốn và nguy hiểm hơn là có thể dẫn đến rủi ro thanh khoản.

◆ **Mức độ các rủi ro trên tùy thuộc vào loại hình dịch vụ trực tuyến mà ngân hàng đang cung cấp. Theo cấp độ từ thấp đến cao, ta có thể phân ra làm ba loại:**

- *Dịch vụ cung cấp thông tin*: Đây là hình thức cơ bản nhất của dịch vụ Internet trực tuyến, là hình thức giao dịch một chiều trong đó thông tin được ngân hàng cung cấp cho khách hàng thông qua website. Đối với loại hình dịch vụ này, rủi ro tương đối thấp và dễ khắc phục; tuy nhiên, ngân hàng cần đảm bảo một sự giám sát liên tục vì những trang web thường là mục tiêu bị tấn công thường xuyên, thông tin gốc bị hư hại.

- *Dịch vụ trao đổi thông tin*: Khách hàng có thể giao dịch tạo tài khoản và điền vào các biểu mẫu của ngân hàng để đăng kí sử dụng dịch vụ hoặc mua các sản phẩm dịch vụ của ngân hàng. Việc đăng kí được thực hiện qua website của ngân hàng trên Internet. Rủi ro gắn liền với loại hình dịch vụ này phụ thuộc vào việc đường truyền website của ngân hàng có được bảo mật tốt hay không, có được kết nối trực tiếp với mạng nội bộ của ngân hàng hay không. Đồng thời cũng phụ thuộc vào độ tin cậy của phần mềm ứng dụng cho phép khách hàng truy cập.

- *Thực hiện các giao dịch*: Loại hình dịch vụ này cho phép khách hàng thực hiện các giao dịch trực tuyến, chẳng hạn như: chuyển tiền từ tài khoản này sang tài khoản khác, chuyển tiền thanh toán trong các giao dịch thương mại điện tử... Đây là loại hình dịch vụ có độ rủi ro tiềm ẩn cao nhất, đòi hỏi mức kiểm soát chặt chẽ nhất và là đối tượng dễ bị tấn công nhất trong các loại hình dịch vụ ngân hàng trực tuyến.

CÁC HƯỚNG DẪN QUẢN TRỊ RỦI RO HOẠT ĐỘNG DỊCH VỤ NGÂN HÀNG TRỰC TUYẾN

Thông báo số 98 của Ủy ban Basel Giám Sát Nghiệp Vụ Ngân hàng (Basel Committee on Banking Supervisor) về nguyên tắc quản lý rủi ro dịch vụ ngân hàng trực tuyến:

Ủy ban Basel Giám Sát Nghiệp Vụ Ngân hàng là một Ủy ban thuộc cơ quan quản lý nghiệp vụ ngân hàng, do Thống đốc các NHTW của nhóm các nước G-10 thành lập vào năm 1975. Bao gồm đại diện cấp cao của các cơ quan quản lý nghiệp vụ ngân hàng và các NHTW đến từ Bỉ, Canada, Pháp, Đức, Ý, Nhật Bản, Luxembourgh, Hà Lan ,Thụy Điển, Thụy Sĩ, Anh và Mỹ; thường nhóm họp tại Ngân hàng Thanh toán Quốc tế ở Basel.

Qua nghiên cứu, Ủy ban Basel nhận thấy: mặc dù các biện pháp quản trị rủi ro truyền thống vẫn phát huy tác dụng đối với hoạt động ngân hàng trực tuyến, chúng cần phải được điều chỉnh, làm cho phù hợp và đôi khi thậm chí cần được nhấn mạnh và mở rộng để có thể đáp ứng những thách thức trong việc quản trị rủi ro dịch vụ ngân hàng trực tuyến. Trên cơ sở đó, Ủy ban Basel Giám Sát Nghiệp Vụ Ngân hàng đã xác định và đưa ra 14 nguyên tắc quản trị rủi ro đối với hoạt động ngân hàng điện tử (*14 Risk Management Principles for Electronic Banking*) nhằm giúp các tổ chức Tài chính Ngân hàng mở rộng chính sách quản trị rủi ro của họ đến một phạm vi rộng lớn hơn, bao quát hơn, có thể quản trị những rủi ro đặc thù của hoạt động ngân hàng điện tử.

Đây không phải là những yêu cầu chính xác, những điều kiện bắt buộc hay những "thông lệ tốt nhất" (*best practice*) như người ta vẫn thường gọi; bởi Ủy ban Basel cho rằng đưa ra yêu cầu chi tiết đối với một hoạt động như hoạt động ngân hàng trực tuyến nhiều khả năng sẽ dẫn đến phản tác dụng. Vì vậy, đây được xem là những hướng dẫn (*guidance*) và mong muốn (*expectations*) mà các ngân hàng có thể áp dụng nhằm phát

triển và điều hành hoạt động ngân hàng trực tuyến an toàn và hiệu quả.

14 nguyên tắc trên của Ủy Ban Basel có thể được tóm gọn thành 3 phần:

1. Sự giám sát của Hội đồng Quản trị và Ban Giám đốc

Với trách nhiệm hoạch định chiến lược phát triển và giám sát rủi ro của tổ chức một cách hữu hiệu, Hội đồng Quản trị và Ban Giám đốc các tổ chức Tài chính – Ngân hàng cần ban hành các văn bản quy định những loại hình dịch vụ ngân hàng trực tuyến mà tổ chức cung cấp và các bước triển khai nó. Trong đó cần thiết chỉ ra những rủi ro cụ thể mà tổ chức có thể gặp phải khi thực hiện hoạt động này, cùng với biện pháp cụ thể phòng ngừa và khắc phục rủi ro. Vai trò quản trị rủi ro của Hội đồng Quản trị và Ban Giám đốc còn thể hiện ở hành động kiểm tra và phê duyệt các quy trình bảo mật quan trọng như việc phát triển và duy trì hệ thống cơ sở hạ tầng, qua đó, dữ liệu và hệ thống dịch vụ ngân hàng điện tử được bảo vệ phù hợp trước những đe dọa từ bên trong và bên ngoài. Nó cũng bao hàm việc ban hành các quy định về mức độ phụ thuộc của tổ chức Tài chính – Ngân hàng với bên thứ ba cung cấp dịch vụ kỹ thuật cũng như dịch vụ outsourcing ngân hàng.

2. Các biện pháp bảo mật

Mặc dù công tác bảo vệ khách hàng ở các tổ chức Tài chính – Ngân hàng có thể khác nhau, song tất cả đều phải đảm bảo làm cho khách hàng hài lòng về vấn đề bảo mật thông tin, bảo vệ dữ liệu của khách hàng, bảo vệ tài sản của khách hàng giống như khi họ sử dụng dịch vụ ngân hàng truyền thống với các kênh phân phối truyền thống. Để hạn chế rủi ro pháp lý và rủi ro uy tín đến mức thấp nhất, các ngân hàng cần giới hạn các thông tin được phép đăng tải trên website, thực hiện phân quyền và nhận dạng các truy cập vào hệ thống, kiểm soát việc truy cập vào hệ thống bằng các biện pháp luận lý và vật lý, xây dựng cơ sở hạ tầng phù hợp cho công tác bảo mật.

3. Ngăn ngừa rủi ro hoạt động, rủi ro pháp lý và rủi ro uy tín

Nhằm bảo vệ mình khỏi hệ quả gia tăng các loại rủi ro trên do cung cấp dịch vụ ngân hàng trực tuyến, các Ngân hàng cần chắc rằng hệ thống kỹ thuật của mình có thể đảm bảo tính chính xác, nhanh chóng và tiện lợi, đáp ứng nhu cầu khách hàng tại mọi thời điểm và vào mọi hoàn cảnh; đảm bảo đưa các dịch vụ trực tuyến đến người sử dụng cuối cùng. Do đó, các ngân hàng cần có biện pháp, chính sách đảm bảo khả năng hoạt động trực tuyến liên tục, nhất quán. Cơ cấu phản ứng với các tình huống bất ngờ (bao gồm cả việc bị tấn công từ bên trong lẫn bên ngoài) cũng rất quan trọng trong việc giảm thiểu các rủi ro hoạt động, rủi ro pháp lý và rủi ro uy tín cho ngân hàng.

Các nguyên tắc của cơ quan tiền tệ Singapore.

Hướng dẫn về kỹ thuật và quản lý rủi ro trong dịch vụ ngân hàng trực tuyến do Cơ quan tiền tệ Singapore ban hành tháng 06-2003 đề ra các biện pháp và nguyên tắc quan trọng nhằm đảm bảo tính bảo mật và độ tin cậy của hệ thống sử dụng Internet ngân hàng khỏi những rủi ro bị tấn công từ bên ngoài cũng như bên trong. Một số biện pháp quản trị rủi ro điển hình do Cơ quan tiền tệ Singapore nêu ra có thể kể đến là:

1) Quản trị nguồn nhân lực: Nội dung gồm ba nguyên tắc cơ bản:

- Nguyên tắc kiểm tra chéo (*never alone*): Các chức năng, thủ tục quan trọng và nhạy cảm của hệ thống cần được thực hiện bởi ít nhất hai người. Bao gồm việc nhập dữ liệu vào hệ thống, cấu hình bảo mật của mạng, thay đổi các thông số hoạt động của hệ thống, xây dựng các bức tường lửa, xây dựng kế hoạch phản ứng với các tình huống bất ngờ... tất cả đều phải đảm bảo nguyên tắc kiểm tra chéo.

- Nguyên tắc phân quyền: Đây là một thành tố quan trọng của hệ thống kiểm soát nội bộ. Các chức năng trong đó trách nhiệm và nghĩa vụ cần được phân chia và thực hiện bởi các nhóm khác nhau, bao gồm: vận

hành hệ thống, thiết kế và phát triển hệ thống, lắp đặt chương trình bảo trì hệ thống, quản lý máy tính và bảo mật hệ thống.

- Nguyên tắc kiểm soát việc truy cập hệ thống:

Quyền truy cập vào hệ thống được cấp phát căn cứ trên phạm vi công việc và mức độ cần thiết của việc truy cập để hoàn thành trách nhiệm.

Chỉ những nhân viên có thẩm quyền phù hợp mới được phép truy cập các thông tin mật và sử dụng các dữ liệu của hệ thống cho các mục đích chính đáng. Không ai có thể nhờ vào địa vị trong tổ chức mà có đặc quyền truy cập những trình ứng dụng hoặc dữ liệu mật ngoài phạm vi công việc của mình.

- Bức tường lửa:

Bức tường lửa là một yếu tố chủ chốt trong bảo mật hệ thống mạng, nhằm cách ly hệ thống mạng nội bộ của ngân hàng với Internet. Tất cả các thông tin trao đổi đều phải chịu sự sàng lọc và kiểm soát. Lỗi hệ thống thường gặp là cho phép kết nối vào Internet mà không qua firewall.

2) Các biện pháp bảo mật:

Ví dụ như:

- Sử dụng máy quét mạng, thiết bị phát hiện và báo động xâm nhập.

- Lắp đặt phần mềm chống virus.

- Thiết lập các quy trình kiểm soát tính bảo mật và giám sát hệ thống mạng.

- Thường xuyên kiểm tra sự bảo toàn của hệ thống mạng và dữ liệu.

- Phân tích nhật kí truy cập để phát hiện các giao dịch và nỗ lực xâm nhập bất ngờ.

3) Lưu trữ dữ liệu dự phòng:

Sự ưu tiên cho phục hồi và duy trì hoạt động cần được xác định. Các thủ tục phản ứng với các tình huống bất ngờ cũng cần được chạy thử và kiểm tra nhằm giảm thiểu sự gián đoạn hoạt động của ngân hàng khi có sự cố.

Ngân hàng cần thiết lập một địa điểm phụ tách biệt khỏi trụ sở chính để lưu trữ dữ liệu và những thông tin quan trọng giúp duy trì hoạt động trong trường hợp trụ sở chính gặp sự cố.

4) Đào tạo khách hàng:

Sự tin tưởng của khách hàng vào độ tin cậy của các dịch vụ ngân hàng trực tuyến tùy thuộc vào sự hiểu biết và sự tuân thủ của họ đối với các biện pháp bảo mật của hệ thống. Việc đào tạo khách hàng bao gồm đào tạo trực tuyến qua trang web hoặc đưa ra những kinh nghiệm, chỉ dẫn cách tiếp thu kiến thức cho khách hàng. Nhằm nâng cao hiểu biết về tính bảo mật, các ngân hàng cần nhấn mạnh với khách hàng sự cần thiết phải bảo mật số CMND, ID, password... và các tài liệu cá nhân quan trọng khác của họ.

Ở Việt Nam hiện nay, NHNN đã ban hành Thông tư số 09/2003 ngày 05-08-2003 hướng dẫn các Ngân hàng trong việc quản lý, cung cấp và sử dụng Internet để truy cập vào mạng. Bao gồm các quy định như:

- Thống đốc NHNN sẽ cho phép các ngân hàng cung cấp dịch vụ của mình qua Internet với điều kiện họ có một mạng lưới máy tính được kiểm soát hiệu quả.

- Ngân hàng phải thành lập một Ủy ban điều hành việc quản lý và sử dụng hệ thống thông tin mạng nội bộ và quốc tế....

Trên đây chỉ là các hướng dẫn mang tính chất định hướng. Trong khi đó các rủi ro do hoạt động dịch vụ ngân hàng điện tử đem lại trên thực tế lại rất cụ thể, phong phú và khó tiên liệu, đặc biệt trong thời kỳ phát triển không ngừng của công nghệ kỹ thuật. Thực tế uy tín ngân hàng bị ảnh hưởng, lợi ích khách hàng bị thiệt hại do giao dịch trực tuyến đã từng xảy ra. Để đảm bảo hiệu quả và tính năng ưu việt của dịch vụ trực tuyến, các ngân hàng cần ra sức nâng cao chất lượng hoạt động kiểm soát rủi ro của mình dựa trên các khung hướng dẫn trên. Xây dựng cơ chế định lượng rủi ro, quản trị rủi ro phù hợp, các biện pháp ngăn ngừa rủi ro cụ thể... là những việc làm cần thiết cho ngân hàng khi quyết định tham gia cung ứng dịch vụ ngân hàng trực tuyến ■