اصول مدیریت ریسک در بانکداری الکترونیک

حسن شرافت نژاد

اشاره

تداوم نوآوری‌های تکنولوژیکی و رقابت بین بانک‌های موجود و بانک‌ها یا صندوق‌های مالی جدید، ارایه گستره وسیعی از محصولات و خدمات بانکداری به مشتریان خرد و کلان را از طریق کانال الکترونیکی میسر ساخته است. این کانال که به آن بانکداری الکترونیک (banking-E) گفته می‌شود، به سرعت در حال توسعه است. انتقال الکترونیکی مبالغ، از جمله پرداخت‌های ریز و سیستم‌های یکپارچه مدیریت نقدینگی و همچنین استفاده از دستگاه‌های خودپرداز برای برداشت وجه و کنترل حساب شخصی، همه بخشی از بانکداری الکترونیک هستند. از سویی دیگر، پذیرش گسترده اینترنت به عنوان کانال ارایه محصولات و خدمات بانکداری هم برای بانک ها و هم برای مشتریان، فرصت‌های جدید بازرگانی را فراهم آورده است، ولی این روند صعودی در کنار مزایا و فوایدی که دارد، خطراتی را نیز به همراه دارد. چنین ریسک‌هایی را مطابق با خصوصیات و چالش‌های اصلی خدمات بانکداری باید شناخت و مدیریت کرد. این خصوصیات، سرعت بی‌سابقه تغییر مربوط به نوآوری خدمات تکنولوژیکی و مشتری، ماهیت فراگیر و جهانی شبکه‌های باز الکترونیکی، تلفیق عملکردهای بانکی با سیستم‌های کامپیوتری و وابستگی روزافزون بانک‌ها به اشخاص ثالث را که اطلاعات لازم را فراهم می‌آورند، شامل می‌شود.

با توجه به اهمیت کنترل، هدایت و مدیریت ریسک‌های ناشی از تحولات و کاربردهای الکترونیکی در بانکداری، این مقاله به بررسی اصول مدیریت ریسک (Risk Management) در بانکداری الکترونیک می‌پردازد.

مدیریت ارشد و هیأت مدیره بانک، مسوول توسعه استراتژی بازرگانی نهاد بانکی است.

چالش‌های مدیریت ریسک

ویژگی‌های اساسی بانکداری الکترونیک (و به طور کلی، تجارت الکترونیک) چند چالش را در زمینه مدیریت ریسک ایجاد می‌نماید:

● سرعت تغییرات مربوط به نوآوری خدمات تکنولوژیکی و خدمات به مشتری در بانکداری الکترونیک بی سابقه است. عملیات جدید بانکی در دوره‌های نسبتاً طولانی و پس از آزمون دقیق به انجام رسیده‌اند. با این حال، امروزه بانک‌ها فشار رقابتی شدیدی را تحمل می‌کنند تا عملیات تجاری جدید را در قالب‌های زمانی بسیار فشرده انجام دهند. در این عرصه رقابتی، ارزیابی راهبردی، تجزیه و تحلیل ریسک و بررسی‌های امنیتی قبل از اجرای عملیات، از جمله عوامل تعیین‌کننده هستند.

● انجام امور بانکی از طریق سایت بانک‌ها و معاملات خرد و کلان به صورت On-line امکان اجرای معاملات مستقیم الکترونیکی و متعاقباً کاهش میزان خطای انسانی را که جزیی از امور یدی است، فراهم می‌آورد. در عین حال، لزوم طراحی سیستم‌های بی‌نقص و قابلیت اجرایی بین سیستمی و درجه‌بندی عملیاتی افزایش می‌یابد.

● بانکداری الکترونیک، وابستگی به فنآوری اطلاعات و در نتیجه، پیچیدگی فنی بسیاری از مسایل عملیاتی و امنیتی و روندی به سمت شراکت، اتحاد و توافقات با اشخاص ثالثی را که اغلب کنترل نشده‌اند، افزایش می‌دهد. این روند توسعه، منجر به ایجاد مدل‌های جدید تجارت می‌شود که بانک‌ها و تشکل‌هایی با ماهیت بانکی مثل شرکت‌های مخابراتی، کمپانی‌های فراهم آورنده خدمات اینترنتی و تکنولوژیکی را در خود جای می‌دهد.

● اینترنت، فراگیر است و ماهیتی جهانی دارد؛ شبکه‌ای باز که در دسترس اشخاص ثالثی در سراسر جهان است، با پیام‌هایی که از مکان‌هایی ناشناخته و از طریق دستگاه‌های بی‌سیم (Wireless) سریع ارسال می‌شوند. بنابراین، اهمیت کنترل امنیتی، روش‌های تأیید صلاحیت مشتری، حفاظت داده‌ها و شیوه‌های حسابرسی و استانداردهای اطلاعات محرمانه مشتریان بیشتر می‌شود.

اصول مدیریت ریسک

اصول مدیریت ریسک در بانکداری سنتی، برای فعالیت‌های بانکداری الکترونیک هم قابل اعمال هستند، ولی ویژگی‌های پیچیده شبکه اینترنت، به کارگیری این اصول را مستلزم سازگاری آنها در تناسب با فعالیت‌های

بانکداری On-line و چالش‌های مدیریت ریسک مربوط به آن می‌نماید. بدین منظور، یکی از اقدامات ضروری در مدیریت بانکی باید بازنگری و اصلاح سیاست‌ها، خط‌مشی‌ها و فرآیندهای مدیریت ریسک کلیه فعالیت‌های کنونی و مورد بررسی بانکداری الکترونیک باشد. البته بانک‌ها برای تمامی فعالیت‌هایشان باید روش منسجم مدیریت ریسک را دنبال کنند و مدیریت ریسک در اجرای عملیات بانکداری الکترونیک هم بخش لازم برای کل شبکه مدیریتی نهاد بانکی است. در جهت تسهیل این روند، بانک‌ها نیاز به اصول مدیریت ریسک دارند تا به آنها کمک کند که سیاست‌ها و روش‌های نظارت ریسک را در بانکداری الکترونیک توسعه دهند و ارایه مطمئن و بی‌نقص الکترونیکی محصولات و خدمات بانکی را ارتقا بخشند. البته این اصول چیزی فراتر از مقررات لازم‌الاجرا هستند، چرا که باید با سرعت تغییر ناشی از نوآوری‌های فنی و تولیدی، تغییر یابند و سازگار شوند.

بانک‌ها نیاز دارند که روش‌های مدیریت ریسک متناسب با ساختار عملیاتی، شرح حال ریسک در بانک، فرهنگ حکومت واحد و در سازگاری با الزامات مدیریت ریسک و خط‌مشی‌های تبیین شده از سوی بازرسان بانکی در قضاوت‌های خاص آنان را تدوین کنند.

از سویی دیگر، با تداوم تعامل صنعت با مسایل فنی بانکداری الکترونیک، از جمله چالش‌های امنیتی، انواع راه‌حل‌های مبتکرانه و با صرفه مدیریت ریسک به این عرصه وارد می‌شوند. این راه‌حل‌ها، به این واقعیت می‌پردازند که بانک‌ها از لحاظ اندازه، پیچیدگی و فرهنگ مدیریت ریسک متفاوتند و سیستم بازرسی آنها از لحاظ چهارچوب‌های قانونی و مقرراتی تفاوت دارد. شرح حال ریسک هر بانک هم متفاوت است و روش تعدیل ریسکی متناسب با میزان عملیات بانکداری الکترونیک، موجودیت ریسک‌های موجود و تمایل و توانایی نهاد بانکی به مدیریت این ریسک‌ها را ایجاب می‌کند.

اصول مدیریت ریسک در بانکداری الکترونیک

اصول مدیریت ریسک در بانکداری الکترونیک را می‌توان در سه دسته طبقه‌بندی نمود: برخی از اصول به نظارت مدیریت و هیأت مدیره مربوط می‌شوند؛ بعضی از اصول در دسته کنترل امنیتی قرار دارند و برخی دیگر در زمره مدیریت ریسک در حیطه علم حقوق و حسن شهرت بانک قرار می‌گیرند.

۱) نظارت مدیریت و هیات مدیره: مدیریت ارشد و هیأت مدیره، مسوول توسعه استراتژی بازرگانی نهاد بانکی است. قبل از ارایه هر گونه خدمات تجاری بانکداری الکترونیک، باید تصمیمات راهبردی روشنی اتخاذ شوند و انسجام این خدمات با اهداف راهبردی واحد، آنالیز ریسک در اجرای فعالیت‌های پیشنهادی، تعدیل (Mitigation) مناسب ریسک و اجرای روش‌های کنترل ریسک‌های مشخص شده و بازنگری مداوم به منظور ارزیابی نتایج فعالیت‌های بانکداری الکترونیک، در دستور کار مدیریت قرار دارند. همچنین ابعاد ریسک عملیاتی و امنیتی استراتژی‌های تجاری بانک‌ها باید به طور کامل در نظر گرفته شوند.

● **اصل ۱-** هیأت مدیره و مدیریت ارشد باید نظارت موثر مدیریتی را بر ریسک‌های مربوط به فعالیت‌های بانکداری الکترونیک اعمال نمایند. بدون بررسی پیشاپیش استراتژیکی و ارزیابی مستمر، بانک در معرض خطر برآورد

امروزه هکرها با استفاده از دستگاه‌هایی به نام Sniffer و روش Spoofing، خود را به جای مشتریان واقعی جا می‌زنند.

کم هزینه یا برآورد اضافی درآمد قرار می‌گیرد. بانک نباید وارد عرصه جدید فنآوری بانکداری الکترونیک شود، مگر اینکه بررسی‌های کارشناسی متناسب با ماهیت و پیچیدگی آن عملیات یا فنآوری به شکلی پویا انجام شده باشد. مدیریت بانک، باید ظرفیت ریسک سازمان بانکی را در رابطه با بانکداری الکترونیک به طور واضح تبیین نماید، روش‌های اصلی گزارش‌دهی و تفویض، از جمله شیوه‌های گسترش برای رویدادهای موثر بر امنیت و حسن شهرت بانک (مثل نفوذ شبکه‌ها، استفاده نادرست از امکانات کامپیوتری و ...) را تعیین نماید، فاکتورهای ریسک مربوط به امنیت، یکپارچگی و موجود بودن محصولات و خدمات بانکداری الکترونیک را بشناسد و اشخاص ثالث تأمین کننده سیستم‌ها یا عملیات کلیدی از بیرون بانک را ملزم به انجام اقدامات مشابهی کند.

بسته به حوزه و پیچیدگی فعالیت‌های بانکداری الکترونیک، حوزه و ساختار برنامه‌های مدیریت ریسک متغیر هستند. منابع لازم برای نظارت بر خدمات بانکداری الکترونیک نیز با کارآمدی و دقت تجارت سیستم‌ها، آسیب‌پذیری شبکه‌ها و حساسیت اطلاعات قابل انتقال باید برابری کند.

● **اصل ۲-** هیأت مدیره و مدیریت ارشد باید جنبه‌های کلیدی فرآیند کنترل امنیت بانک را بررسی و تأیید نماید. هیأت مدیره باید بر توسعه و نگهداری زیربنای کنترل امنیتی نظارت نماید تا این نظام، سیستم‌ها و داده‌های بانکداری الکترونیک را در برابر تهدیدهای داخل و خارج از بانک محافظت نماید. این امر باید شامل تعیین امتیازات اختیاردهی، کنترل‌های دسترسی منطقی و فیزیکی و امنیت کافی زیربنا باشد تا مرزها و محدودیت‌های مناسب در برابر کاربران داخلی و خارجی حفظ شوند.

محافظت از دارایی بانک، یکی از مسوولیت‌های اصلی مدیریت است، ولی در محیط در حال توسعه بانکداری الکترونیک، به خاطر ریسک‌های امنیتی پیچیده مربوط به شبکه جهانی اینترنت و استفاده از فنآوری نوآورانه، این کار سخت‌تر شده است. بنابراین، مدیریت باید روش جامع امنیتی شامل خط‌مشی‌ها و سیاست‌ها را تدوین و اعمال نماید تا خطرات بالقوه‌ای که از داخل و خارج سیستم بانک را تهدید می‌کنند، تحت کنترل قرار گیرند. عناصر اصلی روش موثر امنیتی در بانکداری الکترونیک، شامل انتصاب مدیریت مسوول در نظارت بر سیاست‌های امنیتی واحد، جلوگیری از دستیابی عوامل غیرمجاز به محیط کامپیوترها، داده‌ها و عملیات بانکداری الکترونیک، آزمایش و بررسی مداوم امکانات امنیتی و به روز کردن نرم‌افزارهای مناسب است.

● **اصل ۳-** هیأت مدیره و مدیریت ارشد باید با جدیت، روش نظارت جامع و مناسبی را برای مدیریت روابط بانک با منابع خارج از بانک و وابستگی به اشخاص ثالثی که بانکداری الکترونیک را حمایت می‌کنند، اعمال نماید و توانایی و اعتبار مالی اشخاص ثالث، انجام تعهدات مبنی بر قرارداد و پیروی از استانداردهای امنیتی بانک در شراکت ها و قراردادهای بین بانک را کنترل نماید.

۲)کنترل‌های امنیتی: استحکام تمامی روش‌های کنترل امنیتی که ذکر شدند، به مدیریت خاصی نیاز دارد، زیرا چالش‌های امنیتی ناشی از بانکداری الکترونیک افزایش یافته است. در این زمینه، تایید، یکپارچگی داده‌ها، تفکیک وظایف، کنترل اختیارات، نظارت بر روش‌های حسابرسی و محرمانه بودن اطلاعات بانکی از مسایل اصلی بشمار می روند.

● **اصل ۴-** بانک‌ها باید از روش‌های مطمئن در تأیید (Authentication) هویت مشتریان استفاده کنند، در غیر این صورت، اشخاص فاقد صلاحیت به حساب‌ها دسترسی پیدا می‌کنند و ضرر و زیان مالی و اعتباری به بانک وارد می‌شود. امروزه هکرها با استفاده از دستگاه‌هایی به نام Sniffer و روش Spoofing، خود را به جای مشتریان واقعی جا می‌زنند. بانک‌ها متقابلاً از روش‌های تأیید هویت مثل PINها، رمز ورود، کارت‌های هوشمند، بیومتریک (اثرانگشت، اسکن امضا، اسکن صدا، اسکن شبکیه چشم، اسکن دست) و کارت‌های شناسایی دیجیتالی کمک می‌گیرند. بانک باید تعیین کند که کدام روش تأیید را بر اساس ارزیابی مدیریت ریسک ناشی از سیستم بانکداری الکترونیک انتخاب می‌کند. آنالیز ریسک (Risk Analysis) ظرفیت‌های اجرایی این سیستم (از قبیل انتقال وجه، پرداخت قبض ...)، حساسیت و ارزش داده‌های ذخیره شده و سهولت استفاده از روش تأیید را می‌سنجد. قدرت بانک در این زمینه، میزان بکارگیری از بانکداری الکترونیک را در تجارت‌های بین مرزی افزایش می‌دهد.

● **اصل ۵-** بانک‌ها باید تضمین کنند که وظایف در سیستم‌ها، پایگاه داده‌ها و عملیات بانکداری الکترونیک

سرعت تغییرات مربوط به نوآوری خدمات تکنولوژیکی و خدمات به مشتری در بانکداری الکترونیک بی‌سابقه است.

تفکیک شوند تا خطر کلاهبرداری در عملیات کاهش یابد و دارایی شرکت‌ها و معاملات به درستی تأیید و محافظت شوند.

● **اصل ۶-** بانک‌ها باید از درستی داده‌ها در معاملات، اسناد و اطلاعات بانکداری الکترونیک حمایت کنند، به نحوی که داده‌ها بدون تأیید دستکاری نشوند. بانک‌ها باید اقداماتی را انجام دهند تا صحیح و واقعی و قابل اطمینان بودن معاملات، اسناد و اطلاعات بانکداری الکترونیک در اینترنت یا در پایگاه داده‌های داخلی بانک یا توسط تأمین‌کنندگان خدمات به عنوان شخص ثالث، تضمین شود. در همین رابطه اجرای معامله یا ثبت و دسترسی یا اصلاح سوابق باید به شکلی انجام پذیرد که در برابر دستکاری مقاوم باشد و از اجرای تغییرات غیرمجاز جلوگیری بعمل آورد.

● **اصل ۷-** بانک‌ها باید برای کلیه امور بانکداری الکترونیک، حسابرسی‌های (Audit) بدون ابهام داشته باشند. بدون تردید، ارایه خدمات مالی از طریق اینترنت، اعمال کنترل داخلی و حفظ حسابرسی را دشوارتر می‌کند، البته در صورتی که این اقدامات با محیط بانکداری الکترونیک سازگار نباشند.

● **اصل ۸-** بانک باید محرمانه بودن اطلاعات کلیدی بانکداری الکترونیک را جدی بگیرد و داده‌های سری بانک، تنها توسط افراد و عوامل و سیستم‌های مجاز و تأیید شده قابل دسترسی باشند. بدیهی است که افشای غیر مجاز داده، بانک را در معرض خطر حقوقی و سوء شهرت قرار می‌دهد. استانداردهای بانک برای استفاده و حفاظت از داده‌ها زمانی که اشخاص ثالثی به عنوان تأمین‌کنندگان خدمات از خارج بانک به اطلاعات دسترسی پیدا می‌کنند نیز باید رعایت شوند.

۳)مدیریت ریسک در حیطه قانون و حسن شهرت بانک: در سیستم قضایی هر کشور، قوانین مربوط به حمایت از مشتری و اطلاعات شخصی او خاص همان سیستم هستند.

● **اصل ۹-** بانک‌ها باید اطلاعات کافی را بر روی سایت اینترنتی خود قرار دهند تا به مشتریان این امکان را بدهد که از وضعیت حقوقی و موجودیت بانک قبل از ورود به معاملات الکترونیکی مطلع شوند. نام بانک، موقعیت مکانی آن، هویت مقامات ناظر بانک و نحوه ارتباط مشتری با بانک برای بیان مشکلات، طرح شکایات، موارد سوء استفاده از حساب و سایر اطلاعات حقوقی نیز باید در سایت فراهم شده باشند.

● **اصل ۱۰-** حفظ اطلاعات شخصی مشتریان، اولین وظیفه بانک است. به منظور پشتیبانی از اطلاعات محرمانه هر مشتری، بانک‌ها باید تلاش کنند تا سیاست‌ها و استانداردهای بانک با قوانین قضایی همخوانی داشته باشد و مشتریان هم از این سیاست‌ها آگاه باشند.

● **اصل ۱۱-** بانک‌ها باید برنامه‌های پاسخگویی مناسبی داشته باشند تا مشکلات ناشی از حوادث غیر منتظره، از جمله اتفاقات مخل ارایه خدمات بانکداری الکترونیکی را مدیریت کنند و آنها را به حداقل برسانند. بانک‌ها، باید برنامه‌های الزام‌آور پاسخ‌دهی هم داشته باشند تا سیستم‌ها و خدمات بانکداری الکترونیک را در سناریوها، داد و ستدها و موقعیت‌های جغرافیایی مختلف بهبود بخشند و مکانیسم‌هایی را توسعه دهند که بحران را در زمان وقوع شناسایی کرده، شدت آن را ارزیابی نموده و ریسک همراه با هر نوع اختلال در ارایه خدمات را کنترل کنند. بانک‌ها همچنین باید راهبرد ارتباطی مناسبی را ایجاد نمایند که به بازار خارجی و رسانه‌های ارتباطی که اشکالات امنیتی، نقص سیستم یا حملات On-line را به وجود می‌آورند، بپردازد. بانک ها باید فورا طرف‌های خارج از سیستم، از جمله مشتریان بانک، بانک‌های دیگر و رسانه‌ها را در مورد هر نوع اختلال در بانکداری الکترونیکی خود یا توسعه فنآوری‌ها و خدمات جدید الکترونیکی مطلع سازند.

محافظت از دارایی بانک، یکی از مسوولیت‌های اصلی مدیریت است و مدیریت باید توجه داشته باشد که چالش‌های امنیتی ناشی از بانکداری الکترونیک افزایش یافته است.