مدیریت ریسک عملیاتی دستگاه‌های خودپرداز

(محاسبات سال ۱۳۹۲)

بیژن بیدآباد[۱] **محمود الهیاری فرد**[۲]

چکیده

تبعات مالی، اقتصادی و اجتماعی بانکداری الکترونیک حاکی از افزایش کارائی و اثربخشی این فناوری دارد، حال آنکه با ورود فناوری اطلاعات در حوزه بانکداری، ریسکها و در نهایت ضرر و زیانهائی نیز متوجه بانکدارن و مشتریان خواهد شد. بانکهای پیشرو و مبتنی بر فناوری در استقرار و ارتقاء Core banking خود یکپارچه‌سازی اطلاعات را حتی به خارج از حوزه منابع سازمانی گسترش داده‌اند، بطوریکه خصوصیات Core banking نظیر پردازش تمامی فرآیندها از ابتدا تا انتها، Real time، ۷×۲۴، قابل توسعه، غیروابسته به سکوی نرم‌افزاری، چند زبانه، چند ارزی، حمایت از مقررات و استانداردهای بین‌المللی، قابلیت بومی شدن و همچنین دارا بودن استانداردهای J2EE و یا NET. را شامل می‌شوند. این راهکارها تقریبا قابلیتهای مشابهی را ارائه می‌نمایند و علاوه بر آن می‌بایست سازوکارهای مدیریت انواع ریسک‌های بانکداری را از جمله ریسکهای عملیاتی بانکداری الکترونیک در ابعاد درون سیستمی همچون قطع و اختلال در سیستمها، متوقف شدن و اختلال در کانالهای دیجیتالی، و یا برون سیستمی چون نفوذهای غیرمجاز به سیستم‌های اطلاعاتی، دزدیده شدن کارتهای بانکی، جعل هویت، Phishing، Pharming، Skimming را شامل شود. این مقاله ضمن بررسی ادبیات نظری مدیریت ریسک عملیاتی بانکداری الکترونیک با مطالعه موردی بانک ملی ایران بعنوان نمونه‌ای از بانکهای تجاری ایران سعی دارد تا هزینه سربار ناشی از توقف دستگاه‌های خودپرداز طی سال۱۳۹۲ شمسی را برآورد نماید. بر اساس نتایج حاصل از این تحقیق بطور متوسط هر دستگاه خودپرداز ۴۵ روز از ۳۶۵ روز سال را بدلائل مختلف فنی چون مربوط به قطع ارتباط مخابراتی (۳۷٪)، قسمت پرداخت (۱۹٪)، چاپگر مشتری (۱۷٪)، چاپگر ژورنال (۱۴٪)، سوپروایزر (۱۰٪) و همچنین کارتخوان (۳٪) متوقف می‌باشد،که هزینه سربار هر تراکنش از طریق دستگاه خود پردازکه ناشی از این توقف می‌باشد به قیمتهای سال ۹۲ معادل۹۳۹ ریال برآورد شده است. مجموع هزینه‌های سربار ناشی از متوقف شدن دستگاههای خودپرداز در سال ۹۲ حدود ۱۱۳۱ میلیارد ریال بالغ می گردد.

کلمات کلیدی: ریسک، ریسک عملیاتی، مدیریت ریسک، فناوری اطلاعات، بانکداری الکترونیک، Phishing، Skimming، Pharming، Core banking

---

[۱] دکتر بیژن بیدآباد، مشاورارشد بانک ملی ایران bijan@bidabad.com http://www.bidabad.com

[۲] کارشناس ارشد اداره کل مدیریت ریسک و برنامه‌ریزی بانک ملی ایران http://www.allahyarifard.ir M_allahyarifard@bmi.ir

مقدمه

مدیریت ریسک از جمله مفاهیم آشنا در بانکدارای است و سابقه آن به زمان شکل‌گیری بانکها بر می‌گردد. بانکهای متعارف از دیر باز در دو بازار مالی فعالیت میکنند. از سوئی بعنوان تقاضاکننده‌گان منابع پولی سپرده‌گذاران و از سوی دیگر بعنوان عرضه‌کننده‌گان منابع اعتباری بشمار میروند. مرتبط بودن محصولات و خدمات بانکی با پول در فعالیتهای واسطه‌گری مالی از یک سو، و سعی و تلاش بمنظور حفظ توان رقابتی در بازار از سوی دیگر ضرورت مدیریت ریسک در موسسه‌های واسطه‌گری مالی را بعنوان رکن اصلی معماری بانکداری نوین تلقی می‌نماید. به بیان دیگر ریسکهای واسطه‌گری از آنجا ناشی می‌شوندکه پول که بصورت بدهی و با ایجاد اعتماد از سپرده‌گذاران دریافت شده است می‌بایست در اختیار تقاضاکنندگان منابع پولی قرار گیرند و این فرآیند همراه با احتمال بروز خطرهائی است که در صورت عدم مدیریت صحیح به ورشکستگی بانکها خواهد انجامید. ریسکهای واسطه‌گری مالی چه در قالب بانکداری سنتی و چه در قالب بانکداری مبتنی بر فناوری ریسکهای متفاوتی را شامل خواهد شد که در متون مربوطه طبقه‌بندی و ذکر گردیده است.[۳] نفوذ فناوری اطلاعات در حوزه بانکداری و ظهور پدیدهٔ بانکداری الکترونیک، مهمترین ریسک در این نوع بانکداری را تحت عنوان ریسک عملیاتی در ادبیات نظری مدیریت ریسک مطرح می‌نماید. مجازی‌سازی، دسترسی آسان با ویژگی همه‌جا و همه وقت، آنی بودن تراکنشها، کپی‌سازی با ارزش مجازی مانند پول الکترونیک، سرقت اطلاعات[۴]، تقلب در اطلاعات کارتها[۵] از جمله ریسکهای فناوری است که می‌بایست در واحد مدیریت ریسک علاوه بر ریسکهای متعارف بانکداری مدیریت شوند. در این مقاله سعی خواهد شد ضمن بررسی و مطالعه ریسکهای عملیاتی در بانکداری الکترونیک، ریسکهای عملیاتی کارتهای بانکی را در ایران بررسی نموده، و شکاف موجود با استانداردهای بین المللی را تحلیل نمائیم.

اصول مدیریت ریسک در کمیته نظارتی بال

بنابر بررسیهای گروه بانکداری الکترونیک EBG[۶] کمیته نظارتی بال عمده چالشهای مدیریت ریسک که ناشی از ویژگیهای بانکداری الکترونیک است بشرح ذیل می‌باشد:

- سرعت تغییر و تحول در بعد فناوری و نوع‌آوری در ارائه خدمت به مشتریان در بانکداری الکترونیک بی‌سابقه است. سابقاً برای بکارگیری یک سیستم در بانکداری زمان نسبتاً طولانی‌تری صرف می‌شد و بعد از ارزیابی ها و آزمونهای دقیق و متعدد نسبت به قبول یا عدم پذیرش آن تصمیم‌گیری می‌شد. بر خلاف گذشته امروزه بانکها بعلت فشار رقابتی ناگزیرند تا از سیستمهای جدیدی که هنوز از تولید آنها چندماهی نگذشته است استفاده نمایند. زیرا افزایش رقابت دغدغه مدیریت را تشدید کرده تا کفایت ارزیابی استراتژیک، تحلیل ریسک و همچنین بررسی امنیتی سیستمها در اولویت بکارگیری سیستمهای جدید در نظر گرفته شوند.

---

[۳] ریسک‌های عمده بانکی در عناوین ریسک بازار، ریسک اعتباری، ریسک نقدینگی، ریسک عملیاتی، ریسک قوانین و مقررات و ریسک عامل انسانی طبقه‌بندی می‌شوند که هرکدام زیرفصلهای متعددی نیز دارند. برای مطالعه بیشتر در این مورد نگاه کنید به:

M. Crouhy, D. Galai, R. Mark (2001), Risk Management, McGraw-Hill.

[4] Phishing

[5] Card skimming

6 The Electronic Banking Group (EBG) of the Basel Committee on Banking Supervision.

- تعامل بین وب‌سایت‌های تراکنشی بانکها با سیستم‌های کسب و کارهای تجاری خرده و عمده فروشی برغم حفظ سیستم‌های رایانه‌ای قبلی برای انجام تراکنشها و تعاملات مستقیم افزایش یافته است. افزایش اینچنین تعاملات و تراکنشهای مستقیم و پردازش مکانیزه آنها موجب کاهش خطاهای انسانی و خطای ذاتی در پردازشهای دستی شده است. از طرف دیگر در حال حاضر وابستگی به سیستم‌های سالم و یکپارچه برای انجام تعاملات و ارتباطات داده‌ای و قابل توسعه بودن آنها بیش از پیش احساس می‌شود.
- بانکداری الکترونیک وابستگی بانکها را به فناوری اطلاعات افزایش داده است. از اینرو پیچیدگی فنی در اکثر سیستم‌های امنیتی و عملیاتی روبه افزایش است، و از اینرو حرکت به سمت مشارکتها و تعاملات و قراردادهای برون‌سپاری با طرفهای سوم که دارای تشکلهای منظم و قانونمند نیستند را گسترش داده است. این توسعه منجر به ایجاد شکلهای جدیدی از کسب و کار شامل بانکها و سایر فعالان از قبیل مهیاکننده‌گان خدمات اینترنتی (ISP)، شرکتهای مخابرتی و سایر موسسات فناوری شده است.
- فراگیری و جهانی بودن اینترنت امری ذاتی و اجتناب ناپذیر است. این شبکه باز از سوی افراد ناشناس و از هر مکانی قابل دسترس می‌باشد. به بیان دیگر امکان ارسال پیام از هر جایی و از طریق تجهیزات بدون سیم نیز میسر است. بنابراین نظارتهای امنیتی، فناوریهای احراز هویت مشتریان[۷]، حفاظت از داده[۸]، شیوه‌های بازرسی و ردگیری[۹] و همچنین استانداردهای اختفاء مشتریان[۱۰] بطور معنی‌داری مهم هستند.

اصول مدیریت ریسک به سه بخش عمده و بعضاً مشترک قابل تفکیک می‌باشد که عبارتند از[۱۱]:

- نظارت مدیریت و هیئت مدیره[۱۲] (اصول ۱ تا ۳):
  ۱. نظارت موثر مدیریت در فعالیتهای بانکداری الکترونیک[۱۳]
  ۲. استقرار فرآیندهای نظارت جامع امنیتی[۱۴]
  ۳. تلاش مناسب فراگیر و فرآیندهای نظارت مدیریت در ارتباطات برونسپاری و شرکا[۱۵]
- نظارتهای امنیتی[۱۶]:

۴. احراز هویت در بانکداری الکترونیک

۵. عدم انکار و پاسخگو بودن در مقابل تراکنشهای بانکداری الکترونیک

۶. اقدامات مناسب بمنظور اطمینان از تفکیک وظائف.

۷. نظارتهای مناسب احراز هویت در سیستمها، بانکهای اطلاعاتی و برنامه‌های بانکداری الکترونیک.

۸. یکپارچگی اطلاعات در تراکنشها، رکوردها و اطلاعات بانکداری الکترونیک.

7Customer authentication techniques
[8]Data protection
[9]Audit trail procedures
[10]Customer privacy standards

[۱۱] جهت اطلاع بیشتر مراجعه شود به:http://www.bis.org/publ/bcbs98.pdf

[12]Board and Management Oversight
[13]Effective management oversight of e-banking activities
[14] Establishment of a comprehensive security control process
[15]Comprehensive due diligence and management oversight process for outsourcing relationships and other third-party dependencies.
[16]Security controls

۹. ردگیری مشخص و دقیق تراکنشهای بانکداری الکترونیک.

۱۰. رازداری و محرمانه بودن اطلاعات کلیدی بانک.

- مدیریت ریسک مقررات و شهرت[۱۷]:

۱۱.اطلاع رسانی مناسب از خدمات بانکداری الکترونیک.

۱۲. اختفاء اطلاعات مشتریان.

۱۳. بررسی ظرفیت، استمرار فعالیت، طرحهای در دست اقدام بمنظور اطمینان از در دسترس بودن سیستمها و خدمات بانکداری الکترونیک.

۱۴. راه‌حلها و برنامه‌ها در مدیریت بحران.

بر اساس ماده ۱۳ از رهنمودهای آژانس بانکداری ایالات متحده امریکا برای موسسات مالی که از روشهای اندازه‌گیری پیشرفته[۱۸](AMA) برای محاسبه ریسک عملیاتی استفاده می‌کنند آمده است که عرصه‌های ظهور ریسک عملیاتی بشرح ذیل می‌باشند افزایش استفاده از فناوریهای خودکار، بطور بالقوه موجب انتقال ریسکهای ناشی از خطای فرآیندهای دستی به ریسکهای توقف و خطاهای سیستمی شده که این خطاها ناشی از افزایش اتکاء و اعتماد به سیستمهای جهانی یکپارچه می‌باشد.

- افزایش و گسترش محصولات مبتنی بر فناوریهای پیچیده.
- افزایش تراکنشهای بانکداری الکترونیک و برنامه‌های نرم‌افزاری تجاری مربوط به آن و قرار گرفتن یک موسسه در معرض ریسکهای بالقوه جدید.
- بررسی و آزمون نگهداری حجم وسیعی از اطلاعات، تلفیق، ادغام در قابلیتهای سیستمهای یکپارچه نوین.
- مؤسساتی که بعنوان مهیاکننده‌کنندگان حجم وسیعی از خدمات معرفی می‌شوند نیاز اساسی به عملیات نگهداری در کنترلهای گسترده نظارتی و همچنین فرآیندهای تهیه پشتیبان از اطلاعات خود خواهند داشت.
- توسعه و استفاده از فناوریهای کاهش ریسک (اعم از وثایق، بیمه، اعتبار مشتقه[۱۹]و .....) برغم محافظت از موسسه در مقابل ریسکهای اعتباری و بازار با این حال موسسه را در معرض ریسکهای جدیدی قرار خواهند داد (مانند ریسک مقررات).
- افزایش و توسعه سیستمهای تسویه و تهاتر بانکی[۲۰] که از طریق طرحهای برونسپاری و یا شرکاء فراهم شده‌اند برغم کاهش برخی از ریسکها موجب افزایش سایر ریسکها می‌شوند.

نفوذ فناوری اطلاعات برغم تمامی مزیتهائی که در کسب و کارها از جمله کاهش‌هزینه، مشتری‌مداری، جهانی شدن، افزایش توان رقابتی کسب و کارهای کوچک و متوسط[۲۱](SME)، بهینه شدن تخصیص منابع بر اساس مزیت نسبی و موارد مشابه دیگری از این قبیل بهمراه دارد، احتمال مواجه شدن با برخی ضرر و زیانهای ناشی از بکارگیری و نفوذ فناوری اطلاعات را نیز افزایش خواهد داد که به آن ریسک عملیات بانکداری الکترونیک می‌گویند.

---

[17] Legal and Reputational Risk Management
[18] Advanced Measurement Approaches (AMA)
[19] Credit derivatives
[20] Clearing and settlement systems
[21] Small and Medium Enterprise (SME)

روشهای سوء استفاده در بانکداری الکترونیک

- **جعل عنوان**[۲۲]**:** جعل عنوان از جمله موارد سوءاستفاده بشمار می‌آیدکه از مشخصات شخصی فرد دیگر، مانند نام، شماره ملی، شماره کارت اعتباری بمنظور انجام امور مجرمانه، کلاهبرداری یا سرقت سوءاستفاده شود.
- **بدست‌آوردن حساب**[۲۳]**:** این نوع کلاهبرداری یکی از انواع رایج جعل عنوان می‌باشد بطوریکه شیاد پس از بدست آوردن اطلاعات شخصی، شماره حساب و تغییر آدرس ایمیل رسمی طعمه خود و با ارسال ایمیلی به بانک مبنی بر گم شدن یا دزدیده شدن کارت، تقاضای کارت جدیدی می‌نماید. کارت جدید و صورت حساب برای آدرس جدید ارسال و تا مدتی حساب در اختیار شیاد خواهد بود. این نوع شیادی بیشتر در ارتباط با کارتهای اعتباری می‌باشد.
- **Phishing:** فرآیندی است که متخلف را قادر می‌سازد تا با جلب اعتماد کاربر اطلاعات شخصی، کلمه عبور و همچنین اطلاعات مالی محرمانه را در اختیار فرد شیاد قرار دهد. در این فرآیند اطلاعات در قالب فرمها و با عناوین مختلف از جمله بانک، موسسات وابسته به دولت و غیره برای طعمه ارسال می‌شودو طعمه بدون اطلاع از اینکه فرم دریافتی جعلی (و فقط شبیه فرم اصلی است) ناآگاهانه اطلاعات محرمانه مورد نظر را در آن وارد و برای شیاد ارسال می‌نماید.
- **Pharming:** حمله نفوذگر[۲۴] بمنظور تغییر ترافیک وب سایت به یک وب سایت جعلی دیگر است. در این بخش از شیادی، با دستکاری سرویس دهنده DNS[۲۵] توسط فرد شیاد که در اصطلاح فنی به "سمی"[۲۶] شدن سرویس دهنده DNS کاربر معروف است منجر می‌شود. کاربر به تصور اینکه وارد سایت اصلی بانک می‌شود، وارد سایت جعلی فرد شیاد شده و اطلاعات محرمانه بانکی اعم از شماره حساب، شماره کارت کلمه عبور را وارد می‌نماید و آنگاه فرد شیاد براحتی می‌تواند نسبت به سوء استفاده اقدام نماید[۲۷].
- **تخلفات در دستگاه‌های خودپرداز**[۲۸]: تخلف و شیادی در دستگاه‌های خودپرداز از طریق Skimming، Phishing، Shoulder surfing، جاسازی سیستم‌های کشف اطلاعات[۲۹] و یا دوربین‌های مینیاتوری بمنظور بدست آوردن کلمه عبور[۳۰] و در نهایت از طریق ایجاد کارتهای تقلبی صورت خواهد گرفت.

۱. **Skimming:** فرآیند کپی کردن اطلاعات نوار مغناطیسی کارت اعتباری مشتری از طریق کشیدن کارت از میان کارت‌خوان و استفاده از اطلاعات جهت ساخت کارت تقلبی توسط فرد شیاد را Skimming گویند**.** بطور کلی

---

[22] Identify theft
[23] Account Takeover
[24] Hacker

[۲۵] Domain Name System (DNS): نرم‌افزاری است که دارای بانک اطلاعاتی برای تغییر نام سرویس‌دهنده‌ها در محیط اینترنت به آدرس IP آنها می‌باشد، زیرا از آنجا که آدرس IP در استاندارد IPv6 از چهار قسمت ۳۲ بیتی تشکیل شده که هر بخش از بخش دیگر بوسیله یک نقطه جدا می‌شود و ارقام هر بخش بین ۰ تا ۲۵۵ قابل تغییر است از اینرو بخاطرسپاری این عبارت توسط کاربر مشکل است. کاربر آدرس کامپیوترها در محیط اینترنت را با عبارات روشن و معنادار بکار می‌برد و آنگاه DNS مسئولیت تغییر عبارت به آدرس IP را عهده‌دار می‌شود.

[26] Poisoned

[۲۷] جهت اطلاع بیشتر مراجعه شود به:http://en.wikipedia.org/wiki/Pharming

[28] ATM Fraud
[29] Trapping devices
[30] PIN code

در سه موقعیت، اطلاعات محرمانه ممکن است با خطر روبرو شود: **۱.** در مکان و موقعیت داد و ستد ۲. به هنگام فرآیندهای انتقال به منظور اخذ مجوز ۳. در بخش ذخیره سازی اطلاعات.

۲. **Shoulder surfing:** دزیدن کلمه عبور دارنده کارت به هنگام استفاده از دستگاه خودپرداز (EFT/POS) و یا پایانه فروش از طریق نگاه زیرچشمی از بالای کاربر در حین ورود کاراکترها را شامل می‌شود.

۳. **Phishing** در دستگاه‌های خودپرداز (ATM) و همچنین دستگاه پایانه فروش (EFT/POS) با نصب قطعه‌هایی شبیه دستگاه خودپرداز بر روی دستگاه عملاً ذهن صاحب کارت را منحرف می‌کنند که عملیات وی با دستگاه مجاز صورت می‌گیرد. در این حالت نیز سرقت اطلاعات شخصی سپرده‌گذار و ساخت کارت پلاستیکی جعلی و برداشت از طریق این کانالهای توزیع دیجیتالی امکان‌پذیر است. برخی از شیادان[۳۱] با نصب تجهیزاتی در دستگاه‌های خودپرداز در روزهای تعطیل و یا زمانهای کم تردد بطوریکه این تجهیزات از سوی مشتریان کاملا طبیعی بنظر می‌رسند و از طرفی با در اختیار داشتن تجهیزات بی‌سیم[۳۲] و قرار گرفتن در اتومبیل‌های خود نسبت به سرقت شماره کارت و کلمه عبور اقدام می‌نمایند. روش دیگر شیادان نصب دوربین بی‌سیم در اشیاء جانبی نصب شده در نزدیک دستگاه‌های خودپرداز مانند جای بروشور و یا مکان ریختن رسیدهای مشتریان و یا اشیاء دیگر می‌باشد به نحویکه امکان تصویربرداری از صفحه کلید و صفحه نمایش دستگاه خودپرداز وجود داشته باشد. اطلاعات دریافت شده (کلمه عبور و شماره کارت) بصورت بی‌سیم برای رایانه‌های لپ‌تاپ[۳۳] شیادان که در فاصله چند صد متری قرار می‌گیرند ارسال شده و آنها قادر خواهند بود با کپی نمودن کارت مشتریان، وجوه موجود در حساب مشتریان را سرقت نمایند. بر اساس برآورد TOWER GROUP بطور متوسط از هر ۱۵۶۰۰ تراکنش انجام شده از طریق دستگاههای خودپرداز و پایانه‌های فروش (EFT/POS) یکی از آنها مظنون به کلاهبرداری است. حجم تراکنشهای سالانه (۲۰۰۴) از طریق دستگاه‌های خودپرداز و پایانه‌های فروش (EFT/POS) در ایالات متحده آمریکا معادل ۱۷میلیارد تراکنش می‌باشد که در حدود ۱/۱ میلیون تراکنش برداشت آن کلاهبرداری بوده است.

۴. **Lebanese Loop:** شیاد با قرار دادن یک قطعه در مدخل ورودی کارت کارت خوان و قرار گرفتن پشت سر مشتری نسبت به سرقت کارت و کلمه عبور اقدام نمایند. این قطعه لایه رویه آن مثل ورودی دتگاه است و در آن نواری تعبیه شده که اجازه نمی‌دهد کارت داخل قسمتهای درونی دستگاه وارد گردد و با کشیدن لایه بیرونی کارت نیز با آن بیرون می‌آید. در این روش پس از گیر کردن کارت مشتری درون کارت‌خوان و عدم انجام عملیات، مشتری کلیدهای مختلفی را فشار داده و زمانی که مشتری مستأصل می‌شود به پیشنهاد شیاد دوباره کلمه عبور توسط مشتری بمنظور رفع مشکل وارد می‌شود که کلمه عبور کارت در این شرایط سرقت می‌شود. مشتری بنا به پیشنهاد مجدد فرد شیاد بمنظور اطلاع متصدیان امور بانکی از محل خودپرداز دور می‌شود که فرد شیاد نسبت به خروج قطعه به همراه کارت اقدام و از دستگاه خودپرداز دیگر وجوه موجود از حساب مشتری را سرقت می‌نماید.

---

[31] Scammers
[32] Wireless
[33] Laptop

- **Honeypots**: دامهای دیجیتالی‌آگاهی‌دهنده شبکه‌ایی است که بمنظور منحرف شدن حواس کاربر (طعمه) از عملیات ماشینی بسیار مهم و با ارزش در محیط شبکه طراحی شده‌اند. اینگونه از اشیاء دیجیتالی می‌تواند بعنوان اخطاری برای انجام حمله و یا بهره‌برداری از اطلاعات باشند.
- **Keystroke logger:** یک برنامه نرم‌افزاریست که کاربر اینترنت را قادر می‌سازد تا کلیدهای فشرده شده توسط کاربر دیگر (طعمه) اینترنت را مشاهده کند.
- **Sniffing:** بررسی، مشاهده و همچنین ثبت اطلاعات اینتنرتی و ترافیک سایر کاربران اینترنت را گویند.
- **Spoofing:** دریافت Email از سوی فردی شیاد با عنوان جعلی که نشانگر استناد داشتن به یک فرد یا سازمانی است که در واقعیت مربوط به آن مرجع نمی‌باشد و جعل شده است.
- **Synthetic identity:** هویت ساختگی و جعلی دزدیده شده از قسمتهای مختلف.
- **Trojan horses:** برنامه‌ای که از روی بدخواهی و با نیت سوء نوشته شده و آثار زیان‌بار آن مخفی است و به منظور نفوذ در رایانه مورد نظر و از بین بردن اطلاعات طراحی شده است.
- **Freeware:** برنامه‌هایی است که علی الظاهر برای پاسخ به برخی نیازهای کاربران طراحی و بطور مجانی در اینترنت گذاشته شده‌اند و کاربران برای رفع نیاز کاری خود آنها را بارگیری می‌نمایند غافل از اینکه این برنامه‌ها هنگام اجرا وظایف خاصی را برای سازندهٔ آنها انجام می‌دهند.
- **نرم‌افزار جاسوسی**[۳۴]: نرم‌افزاریست که اطلاعات شخصی مشتریان را ردگیری کرده و آنگاه آنرا در اختیار طرف ثالث قرار می‌دهد. این نرم‌افزار در بیشتر موارد با اطلاع روی کامپیوتر نصب و گاهی اوقات با توجه به عدم آگاهی و دانش لازم در کامپیوتر کاربر نصب می‌شود. نمونه‌هائی از نرم‌افزارهای جاسوسی بشرح ذیل می‌باشند:
  ۱. **Adware:** این نرم‌افزار عادات خرید مشتریان را ضبط و دنبال می‌کند.
  ۲. **Web Bugs:** یک نوعی از نرم‌افزار Adware است که اطلاعات مربوط به عادات خرید مشتریان را به طرف ثالث ارسال می‌نماید. طرف ثالث از آن به بعد کنترل کامپیوتر را بعهده دارد و هرگاه لازم باشد می‌تواند به اطلاعات دسترسی پیدا کند.
  ۳. **Proxy Adware:** این نرم‌افزار بر اساس توافق کلیه ترافیک ورودی و خروجی کامپیوتر را از طریق سرورهای مورد نظر تغییر مسیر خواهد داد. این موضوع شامل تمامی اطلاعات حتی اطلاعات رمز نگاری شده توسط پروتکلهای SSL و یا اطلاعات محرمانه شامل کلمات عبور بانکداری Online و همچنین تراکنشهای کارتهای اعتباری را نیز شامل می‌شود.
  ۴. **تروژانها و سایر نرم‌افزارهای مخرب**[۳۵]: تروژانها بطور کلی برای نقل و انتقال کرمها، ویروسها و سایر کدهای خرابکار به سایر کامپیوترها استفاده می‌شوند. بدترین نوع تروژنها را RAT[۳۶] تشکیل می‌دهند. RAT ها موجب می‌شوند تا تمامی کنترل کامپیوترهای شخصی در دسترس نفوذگرها قرار گیرند. تروژانها زمانی در یک کامپیوتر نصب می‌شوند که اطلاعات فرد مورد نظر سرقت شده و آنگاه با ارسال پست الکترونیک و باز شدن آن

[34] Spyware
[35] Trojans and other Malware
[36] Remote Access Tools (RAT)

بطور اتوماتیک در کامپیوتر نصب می‌شود.

راههای جلوگیری

- امنیت شبکه و مرکز عملیات[۳۷]
- تیم واکنش به رخدادهای امنیتی[۳۸] (CSIRT)
- واحد هشدار امنیت داده‌ها[۳۹](DSA) و تشخیص و جلوگیری از حملات ونفوذ[۴۰][۴۱](IPS) ، تصفیه محتوای ترافیک، آنتی ویروس شبکه ای و آنتی اسپم (در بانک)
- سیستم های هویت شناسی[۴۲]، حسابرسی مبتنی بر کاربر، بازرسی حالتمند ترافیک، ترجمه آدرس و پورت NAT/PAT/MAT ، مدیریت پهنای باند (در بانک)
- سیستم ثبت Log متمرکز جهت ثبت رخدادهای گوناگون در سامانه (در بانک)
- استفاده از پروتکل های امن مانند SSL[۴۳] درشبکه خصوصی مجازی (VPN) و IPSec[۴۴] در انتقال داده ها (در بانک)
- بروزرسانی مرتب سیستم‌عامل و Browser.
- جلوگیری از نصب نرم‌افزارهای ناشناخته و نامطمئن.
- مطالعه و بررسی اطلاعات دقیق هر نرم‌افزار قبل از download شدن.
- اخذ گواهی مربوط به اطمینان از نرم‌افزار و قانونی بودن آن از واحد اصلی.
- عدم کلیک لینک‌های معرفی شده در پست الکترونیک بمنظور عدم دسترسی به سایت‌های غیرقانونی و جاسوسی.
- استفاده از فایروالها یا دیواره های آتش بمنظور کنترل ترافیک ورودی و خروجی.

---

[37] Network security and operational center

[38] Computer Emergency Response Team (CSIRT)

[39] Data security alerts (DSA)

[۴۰] جهت تشخیص رفتارهای غیر طبیعی شبکه از رخ دادن حملاتی چون حملات سیل آسا و پویش درگاه جلوگیری میکند، همچنین با استفاده از الگوی حملات با حملاتی چون Back doorها و Exploitها مقابله می‌کند.

[41] Intrusion prevention systems

[۴۲] هویت شناسی: سیستمی است که وظیفه آن مانع سوء استفاده از آدرس IP و آدرس MAC در شبکه های عمومی می‌شود این سیستم می بایست دارای قابلیت های : پشتیبانی از انواع کارگزار راه دور، کنترل دسترسی نشست‌های کاربران مدیریتی و معمولی، تشخیص هویت ترافیک، سیاست‌های گذرواژه برای کاربران مدیریتی و معمولی، سیاست‌های معلق کردن حساب کاربران، پشتیبانی از روش احراز هویت X-Auth برای سرویس IPSec، پشتیبانی از روش احراز هویت802.1X و نظارت لحظه ای بر فعالیت‌های کاربران احراز هویت شده باشد.

[۴۳] اهداف پروتکل SSL عبارتند از: تصدیق اصالت یک سرویس دهنده و یک سرویس گیرنده و ایجاد ارتباط امن و رمزنگاری شده بین سرویس دهنده و سرویس گیرنده.

[۴۴] هدف از معماری IPSec فراهم آوردن امنیت برای اطلاعات عبوری از لایه IP می‌باشد. این پروتکل مبتنی بر رمزنگاری با کیفیت بالا را فراهم می‌کند

جدول ۱: مقایسه آثار انواع ریسکهای فناوری برون سیستمی مجرمانه

ویروس	کرم[۴۵]	تروژان	نرم‌افزار جاسوسی
برنامه‌ایست که خود را به سایر فایلها و یا فایلهای سیستمی متصل می‌کند و از این طریق با گسترش خود از طریق جابجائی فایل یا media و یا تاثیرگذاری بر سکتورهای خاص دیسک سخت نظیر boot sector و یا جدول‌های تخصیص فایل FAT اقدام به فعالیتهای خرابکارانه می نماید.	برنامه‌ایست که قابلیت تکثیر بر روی سایر سیستمها را داشته و اغلب بدون نیاز به دخالت کاربر هنگام آسیب پذیری اجرا شده و اقدام به فعالیتهای خرابکارانه و مزاحم می نماید.	برنامه‌ایست که بطور مستقل انتشار نمی‌یابد و بصورت پنهان اجرا شده و وظائف هدفمندی را انجام می‌دهد. این برنامه غالباً از فقدان آگاهی امنیتی کاربران استفاده نموده و از طریق ظاهر شدن برنامه‌های جذاب (مانند Screen saver، game)، داده (مانند عکس، موسیقی) به کامپیوتر کاربر منتقل می‌گردد.	برنامه‌ایست که به مشاهده فعالیتهای کاربران و کسب اطلاعات مهم مانند کلمه عبور، پیکربندی سیستم و کدهای محرمانه و ارسال آنها به مراکز خاص می‌پردازد. این برنامه اساساً از طریق مشارکت اطلاعات با شخص ثالث از طریق اتصال به اینترنت منتقل می‌شود.

ریسک عملیاتی بانکداری الکترونیک در ایران

رویکرد مکانیزاسیون و نفوذ رایانه‌های شخصی در بانکهای ایرانی به دهه ۱۳۶۰ شمسی برمی‌گردد[۴۶]، شاید تا آن زمان تردیدها و مقاومت‌ها در بکارگیری رایانه‌های شخصی و فرآیندهای مکانیزه بدلیل تبعات ناشی از ریسک عملیاتی و سوء استفاده‌های ناشی از محیط سایبر نبوده بلکه عامل مقاومت درعدم آشنائی با پدیده فناوری اطلاعات و عادت نمودن به فرآیندهای سنتی و اجرائی شدن تمامی فرایندها به روش سنتی بوده است. ریسک عملیاتی بانکداری الکترونیک و ضرر و زیان ناشی از آن با گسترش و توسعه بانکداری الکترونیک اینترانتی و افزایش کانالهای دیجیتالی بدون حضور و مراجعه مشتریان به شعبه نیز از اواخر دهه ۱۳۷۰ شمسی آغاز شده است. طراحی و معماری صحیح سیستم‌های اطلاعاتی نقش مهمی را در موفقیت بانکداری الکترونیک ایفا می‌نمایند بطوریکه فقدان هریک از زیر سیستم‌ها و ماژولها برغم تمامی مزیتها در بکارگیری و ارائه خدمات بانکداری الکترونیک اجرای موفقیت آمیز خدمات و محصولات مبتنی بر فناوری را با شکست روبرو خواهد ساخت. گسترش خدمات و محصولات بین بانکی از طریق شبکه شتاب و راه‌اندازی سیسم تسویه ناخالص آنی (RTGS) بین بانکها از سوی بانک مرکزی و ارائه خدمات برداشت و انتقال وجوه از طریق دستگاه‌های PINPAD و EFT/POS برغم تمامی مزیتها و رضایت مشتریان هنوز سابقهٔ زیادی در بانکداری ایران ندارد و هنوز بسیاری از مسائل مربوط به مدیریت ریسک و سیستمهای نظارتی مکانیزه و مشکلات ناشی از آن برای برخی از

[45] Worm

[۴۶] جهت اطلاعات بیشتر مراجعه شود به الیهاری‌فرد، محمود، "خدمات بانکداری الکترونیک و نیازهای اجرائی آن در مقایسه تطبیقی خدمات مختلف بانکی"، پژوهشکده پولی و بانکی بانک مرکزی ج.ا.ا ، ۱۳۸۴

بانکها و مشتریان هویدا نگشته است. تبعات سوء ناشی از عدم وجود مدیریت ریسک مبتنی بر فناوری برای ردگیری تراکنشها، مانیتور نمودن کانالهای توزیع دیجیتال می‌تواند به افزایش هزینه‌های سربار بانکها منجر و یا حتی ممکن است ارائه خدمات مبتنی بر فناوری را با شکست روبرو سازد. لذا در این بررسی ریسک عملیاتی بانکداری الکترونیک را از دو منظر مورد بررسی قرار می‌دهیم. با انتخاب بانک ملی ایران به عنوان بانک منتخب نخست ریسک عملیاتی ناشی از توقف دستگاه‌های خودپرداز در سال ۱۳۹۲ را بررسی نموده و تبعات مالی آن را برآورد و آنگاه عوامل ایجاد کننده سوءاستفاده و اختلاس در سیستم یکپارچه و کارتهای بانکی را بررسی می‌نمائیم.

انواع خطاهای درون سیستمی

یکی از مهمترین کانالهای توزیع بانکداری الکترونیک دستگاههای خودپرداز (ATM) می‌باشندکه بانکها خدمات مختلفی از جمله پرداخت وجوه، پرداخت صورتحساب و قبوض، گردش مانده و همچنین انتقال وجوه را با استفاده از قابلیتهای این دستگاهها ارائه می‌نمایند. متوسط دستگاه‌های خودپرداز فعال بانک ملی ایران طی سال ۱۳۹۲ مطابق جدول ۲ برابر ۶۴۴۱ دستگاه می‌باشد[۴۷]. براساس این جدول تعداد خطاها و میزان وقفه‌های ناشی از هر یک از خطاها در دستگاههای خودپرداز طی ۱۲ ماه سال ۱۳۹۲ نشان داده شده‌اند. انواع خطاهای مورد بررسی در این تحقیق بمنظور مطالعه تاثیر و محاسبه هزینه‌های سربار ناشی از ریسک فناوری درون سیستمی، محدود به خطاهای دستگاه‌های خودپرداز است که بشرح ذیل میباشند:

- خطای کاستهای دستگاه خودپرداز: شامل کلیه خطاهای مربوط به محل قرار گرفتن انواع اسکناسها و یا اینکه مربوط به برگشت اسکناسهای ناشی از تراکنشهای ناقص می‌باشند. قسمت اعظم این خطا به عدم سرویس‌دهی بموقع مسئولین اجرائی و نظارتی شعب برمی‌گردد.
- خطای چاپگر ژورنال: شامل کلیه خطاهای مربوط به چاپ و تهیه لیست تراکنشهای مشتریان جهت نگهداری در بانک و عملیات مربوط به فرآیندهای حسابداری و رفع مغایرتها می‌شوند.
- خطای چاپگر مشتری: شامل کلیه خطاهای مربوط به چاپگر و تهیه صورتحساب تراکنشها (پنج تراکنش قبلی) و یا رسید مشتری می‌باشند.
- خطای کارت‌خوان: شامل کلیه خطاهای مربوط به قبول کارت و بخشی از تجهیزات دستگاه خودپرداز می‌شود که اطلاعات مربوط به مشخصات دارنده کارت و کلمه عبور را از داخل نوار مغناطیسی خوانده و امکان انجام تراکنش را برای کاربر فراهم می‌نماید.

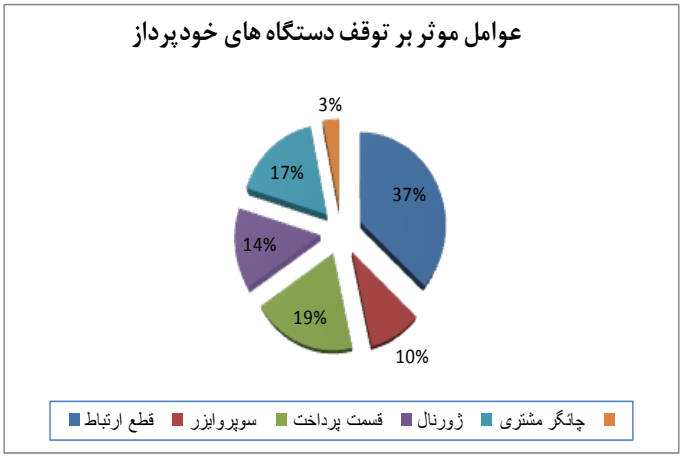
[47] https://ebank.bmi.ir/mbsweb/BankMelli/AppMain.aspx

جدول ۲ : ترکیب وسهم هر یک از خطاها در دستگاه‌های خودپرداز بانک ملی ایران (به ساعت)

تعداد تراکنش [۴۸]	کل خطا ساعت	قطع ارتباط	سوپروایزر	قسمت پرداخت	چاپگر ژورنال ساعت	چاپگر مشتری ساعت	کارتخوان ساعت	تاریخ	تعداد ATM
۹۹/۹۹۸	۵۵۶،۹۰۲	۲۱۶،۶۴۸	۴۵،۸۲۶	۱۰۳،۸۶۳	۸۲،۳۹۱	۸۹،۶۱۲	۱۸،۵۶۲	92/۰۱	6419
۸۶/۱۷۰	۶۳۲،۱۸۴	۲۲۸،۵۱۹	۵۶،۱۶۳	۱۱۳،۵۹۲	۱۰۲،۵۷۲	۱۱۰،۵۴۶	۲۰،۷۹۲	92/۰۲	6424
۷۶/۸۶۰	۶۱۷،۸۶۵	۲۳۲،۵۱۰	۵۴،۵۸۴	۱۱۶،۷۹۳	۹۲،۷۵۲	۱۰۱،۸۸۵	۱۹،۳۴۱	92/۰۳	6428
۷۸/۸۳۰	۶۲۸،۴۲۱	۲۴۳،۶۸۲	۵۶،۶۶۶	۱۱۴،۷۱۶	۹۲،۳۸۷	۱۰۱،۴۴۵	۱۹،۵۲۵	92/۰۴	6432
۸۰/۱۵۸	۶۷۰،۷۱۳	۲۵۹،۲۰۶	۶۳،۹۹۶	۱۲۲،۸۶۰	۹۵،۱۲۴	۱۰۶،۹۳۲	۲۲،۵۹۵	92/۰۵	6434
۸۰/۰۰۹	۶۶۳،۰۳۶	۲۵۴،۳۳۶	۷۷،۱۹۲	۱۱۷،۹۱۷	۸۷،۴۸۵	۱۰۴،۸۸۴	۲۱،۲۲۲	92/۰۶	6439
۱۰۴/۷۱۰	۶۴۵،۲۵۳	۲۴۰،۹۰۴	۷۰،۴۵۴	۱۱۸،۰۲۲	۸۹،۸۴۲	۱۰۵،۵۷۵	۲۰،۴۵۶	92/۰۷	6444
۱۱۵/۰۴۵	۵۷۸،۹۴۹	۲۱۲،۵۵۶	۶۲،۸۳۹	۱۱۳،۰۸۲	۷۹،۳۲۱	۹۴،۲۵۵	۱۶،۸۹۶	92/۰۸	6449
۱۱۵/۲۱۱	۶۱۸،۵۰۶	۲۱۳،۹۸۸	۶۴،۸۴۸	۱۱۸،۸۶۶	۸۳،۸۵۰	۱۱۷،۸۶۸	۱۹،۰۸۶	92/۰۹	6452
۱۰۸/۶۱۲	۵۴۹،۰۰۶	۱۸۹،۷۱۵	۴۷،۳۰۳	۱۱۷،۰۳۶	۶۶،۸۱۵	۱۰۹،۰۷۱	۱۹،۰۶۶	92/۱۰	6454
۱۱۶/۱۸۷	۵۳۱،۶۴۵	۱۷۷،۳۴۳	۴۱،۵۶۶	۱۱۳،۴۰۶	۷۰،۳۶۸	۱۱۰،۵۳۴	۱۸،۴۲۸	92/۱۱	6456
۱۳۱/۰۹۷	۲۶۹،۳۶۱	۹۵،۳۷۰	۲۹،۳۹۴	۶۳،۸۷۵	۳۳،۷۱۱	۳۹،۵۹۵	۷،۴۱۶	92/۱۲	6460
۱۱۹۲/۹	۶،۹۶۱،۸۴۱	۲۵۶۴۷۷۷	۶۷۰۸۳۱	۱۳۳۴۰۲۸	۹۷۶۶۱۸	۱۱۹۲۲۰۲	۲۲۳۳۸۵	مجموع	6441 [۴۹]
۱۸۵۲۰۴ [۵۰]	۱۰۸۱	۳۹۸	۱۰۴	۲۰۷	۱۵۲	۱۸۵	۳۵	سرانه توقف هر ATM (ساعت)	
	۴۵	۱۶/۵۹	۴/۳۴	۸/۶۳	۶/۳۲	۷/۷۱	۱/۴۵	سرانه توقف هر ATM (روز)	

ماخذ: آمارهای داخلی بانک ملی ایران

کلیه خطاهای مورد بررسی به نحوی از انحاء منجربه متوقف شدن دستگاه خودپرداز می‌شود و مشتریان امکان دریافت خدمات بانکی را نخواهند داشت. مطابق با نمودار وقفه‌های دستگاه خودپرداز در بانک ملی ایران از بیشترین به کمترین سهم به ترتیب مربوط به قطع ارتباط مخابراتی (۳۷٪)، قسمت پرداخت (۱۹٪)، چاپگر مشتری (۱۷٪)، چاپگر ژورنال (۱۴٪)، سوپروایزر(۱۰٪) و همچنین کارتخوان (۳٪) می‌باشد.



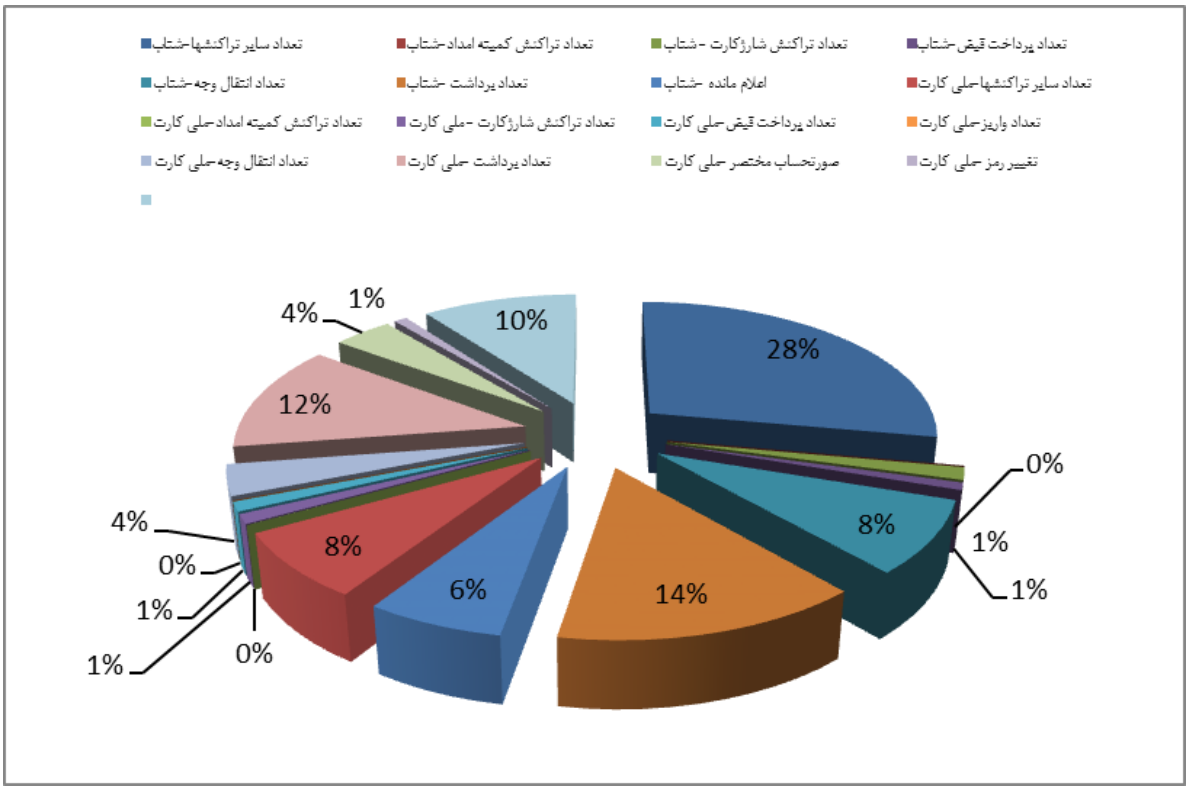
در جدول ۲ همانطور که نشان داده شده است در سال ۱۳۹۲ بطور متوسط ۶۴۴۱ دستگاه خود پرداز فعال در ایجاد ۱۱۹۲/۹ میلیون تراکنش اعم

[۴۸] تعداد تراکنش‌ها به میلیون

[۴۹] متوسط تعداد دستگاه خودپرداز فعال در طول سال

[۵۰] متوسط تعداد تراکنش هر دستگاه خودپرداز در سال

از برداشت وجوه نقد توسط مشتریان بانک (۱۲٪)، برداشت وجوه نقد توسط مشتریان شتاب (۱۴٪)، اعلام مانده ملی کارت (۱۰٪)، اعلام مانده شتاب (۶٪)، انتقال وجه ملی کارت (۴٪)، انتقال وجه شتاب (۸٪)، تعداد پرداخت قبض ملی کارت (۱٪)، تعداد پرداخت قبض شتاب (۱٪)، تعداد شارژ کارت ملی کارت (۱٪)، تعداد شارژکارت شتاب (۱٪) و تعداد سایر تراکنشهای شتاب (۲۸٪) می باشد. کیفیت تراکنشها از طریق دستگاه های خودپرداز در نمودار زیر نشان داده شده است.



جدول ۳: تعرفه کارمزد انتقال وجوه از طریق دستگاه های خودپرداز (ATM)

	نوع خدمت	نرخ کارمزد
	اعلام مانده حساب	از طریق: ATM در مورد تراکنشهای شتابی ۱،۰۰۰ ریال
انتقال وجوه شتابی	تا ده میلیون ریال	۵۰۰۰ ریال
	از ده میلیون ریال تا بیست میلیون ریال	۷۰۰۰ ریال
	از بیست میلون ریال تا سی میلیون ریال	۹۰۰۰ ریال
	از سی میلیون ریال تا چهل میلیون ریال	۱۱۰۰۰ ریال

ماخذ: بخشنامه های صادره بانک

در جدول ۳ تعرفه کارمزد ارائه خدمات از طریق دستگاه های خودپرداز نشان داده شده است. انتقال و جوه بین بانکی از طریق دستگاه های خودپرداز مشمول تعرفه سامانه حواله الکترونیکی بین بانکی (سحاب) می‌باشد.

عدم امکان دسترسی به آمار پراکندگی تراکنشهای مبلغی بین بانکی (تراکنشهای با کار مزد بالا) از طریق دستگاه های خودپرداز دلیلی روشن برای استفاده از روشهای مختلف از جمله توزیع نرمال و یا بر اساس نظر خبرگان می باشد. که در این گزارش بر اساس نظر خبرگان در جدول شماره ۳ استفاده شده است.

بطور کلی ترکیب تراکنش‌ها را می توان بصورت جدول زیر خلاصه کرد که در محاسبات هزینه فرصت ناشی از توقف دستگاه های خودپرداز مورد استفاده قرار می‌گیرند.

جدول ۳: ترکیب کیفی تراکنشها (از نظرکارمزد)

نوع تراکنش	نظر خبرگان	سهم	میانگین وزنی	میزان کارمزد به ازای هر تراکنش
تراکنش بدون کارمزد	–	٪۲۳	٪۲۳	۰ ریال
تراکنش با کارمزد متوسط	–	٪۴۱	٪۴۱	۱۰۰۰ ریال
تراکنش با کارمزد بالای شتابی	٪۱۰	٪۳۶	٪۳/۶	۵۰۰۰ ریال
تراکنش با کارمزد بالای شتابی	٪۱۵		٪۵/۴	۷۰۰۰ ریال
تراکنش با کارمزد بالای شتابی	٪۲۰		٪۷/۲	۹۰۰۰ ریال
تراکنش با کارمزد بالای شتابی	٪۵۵		٪۱۹/۸	۱۱۰۰۰ ریال

ارزیابی و محاسبه هزینه سربار ناشی از توقف دستگاه‌های خودپرداز و تاثیر آن در بهای تمام شده هر تراکنش توسط دستگاه‌های خودپرداز در جدول ۴ نشان داده شده است. همانطور که در جدول ۴ مشاهده می‌شود، به ازای هر تراکنش ۹۳۹ ریال به بهای تمام شده هر تراکنش ناشی از توقفهای سال ۱۳۹۲ از طریق دستگاه‌های خودپرداز اضافه می‌شود. مجموع هزینه‌های سربار ناشی از ریسک عملیاتی توقف دستگاه‌های خودپرداز در سال ۱۳۹۲ برابر ۱۱۳۱ میلیارد ریال می‌باشد. با فرض اینکه قیمت هر دستگاه خودپرداز معادل دویست و پنجاه میلیون ریال باشد با اجرای مدیریت ریسک عملیاتی از محل هزینه سربار ۱۱۳۱ میلیارد ریالی می‌توان در حدود ۴،۵۲۲ دستگاه خودپرداز جدید خریداری نمود که معادل افزایش ٪۷۰ ظرفیت موجود دستگاه‌های خودپرداز بانک ملی می‌باشد.

جدول۴: نحوه محاسبه هزینه‌سربار هر تراکنش ناشی از توقف دستگاه خودپرداز

شرح	
متوسط تعداد دستگاه های ATM فعال در سال ۹۲	۶۴۴۱ عدد
سرانه تعداد تراکنشهای انجام شده هر ATM در سال ۱۳۹۲	۱۸۵،۲۰۴ عدد
هزینه استهلاک هر دستگاه خودپرداز در هر تراکنش (دستگاه ATM سه ساله مستهلک می‌شود)	۴۵۵ ریال
هزینه کارکنان برای هر تراکنش (به ازای هر دستگاه یک نفر)	۳،۶۰۸ ریال
هزینه اجاره و پشتیبانی خطوط به ازای هر تراکنش	۶۵/۳۷ ریال
هزینه‌های ارتباطات و مخابرات هر تراکنش	۲۲۵ ریال
هزینه های مصرف شدنی رایانه‌ای (لحاظ کردن ۱/۳)	۲۹/۹۳ ریال
هزینه تعمیر و نگهداری دستگاه‌های VSAT برای هر تراکنش	۲۵۸ریال
هزینه تعمیر و نگهداری دستگاههای ATM بر اساس قیمتهای سال ۱۳۹۲	۱۳۴
بهای تمام شده هر تراکنش از طریق دستگاه خودپرداز(ATM) بر اساس قیمتهای سال ۹۲	۴،۲۳۵ ریال
بهای تمام شده تراکنشها توسط هر ATM در یک روز (بدون احتساب مانده گیری و انتقال وجوه)، ۵۱۲×۴۲۳۵	۲،۱۶۸،۲۰۸
هزینه فرصت هر ATM بابت تراکنش‌ها با کارمزد متوسط سال ۹۲ در روز ۱۰۰۰×۱۸۶	۱۸۶،۰۰۰ریال
هزینه فرصت هر ATM بابت انتقال وجوه بین بانکی با کارمز ۵۰۰۰ ریالی در سال ۹۲ در روز ۱۸×۵۰۰۰	۹۲،۱۵۵ ریال
هزینه فرصت هر ATM بابت انتقال وجوه بین بانکی با کارمزد ۷۰۰۰ ریالی در سال ۹۲ در روز ۲۸×۷۰۰۰	۱۹۳،۵۲۶ ریال
هزینه فرصت هر ATM بابت انتقال وجوه بین بانکی با کارمزد ۹۰۰۰ ریالی در سال ۹۲ در روز ۳۷×۹۰۰۰	۳۳۱،۷۵۹ ریال
هزینه فرصت هر ATM بابت انتقال وجوه بین بانکی با کارمزد ۱۱۰۰۰ ریالی در سال ۹۲ در روز ۱۰۱×۱۱۰۰۰	۱،۱۱۵،۰۷۸ ریال
مجموعه هزینه فرصت روزانه هر ATM بر اساس قیمتهای سال ۱۳۹۲	۳،۹۰۰،۷۲۶ ریال
هزینه هر ATM طی روزهای توقف، ۴۵×۳،۹۰۰،۷۲۶	۱۷۵،۵۳۲،۶۶۵ریال
هزینه کلیه دستگاه‌های خودپرداز طی روزهای توقف، ۶،۴۴۱×۱۷۵،۵۳۲،۶۶۵	۸۹۵،۸۶۱،۱،۱۳۰،۶۰۵ریال
هزینه سربار هر تراکنش ناشی از توقف دستگاه خودپرداز (در سال۹۲)، ۱،۲۰۴÷۱،۱۳۰،۶۰۶	۹۳۹ ریال

ریسکهای عملیاتی برون سیستمی

سوء استفاده از حسابهای کارت و سیستم یکپارچه از طریق عوامل شیاد و کلاهبردار بخشی از هزینه‌هایی است که با گسترش سیستم‌های یکپارچه در بانکهای ایرانی رونق گرفته است. عدم استقرار Core banking کامل در برخی از بانکهای ایرانی و عدم دسترسی به ماژول مدیریت ریسک، گردش‌کار[۵۱] (WFM)[۵۲] بمنظور ردگیری مکانیزه تراکنشها که اصول ارائه شده توسط EBG کمیته نظارتی بال می‌باشد، موجب ایجاد مغایرتهائی در حسابهای واسطه سیستم‌های یکپارچه و سرقت وجوه از حسابهای کارت برخی از مشتریان شده است. این نوع حسابها در بانکهائی که از چند سیستم غیریکپارچه (شبکه‌های داخلی شعبه) در ارائه محصولات و خدمات به مشتریان استفاده می‌کنند بمنظور ارتباط حسابداری بین دو سیستم در نظر گرفته شده‌اند. این نوع حسابها در پایان عملیات روزانه می‌بایست فاقد مانده بدهکار یا بستانکار باشد.

اختلاس از کارتها و سیستم‌های یکپارچه نیز ناشی موارد متنوعی می‌باشد. سرقت کارت و کلمه عبور توسط شیادان و همچنین سرقت وجوه مشتریان از حسابهای کارت آنها نیز از جمله مواردی است که در سالهای اخیر در بانکهای ایرانی نیز مشاهده شده است. شگردهای شیادان در بانکهای ایرانی ممکن است به روشهای مختلفی صورت پذیرد که از جمله آنهامیتوان به موارد زیر اشاره نمود:

- سرقت کارت و کلمه عبور به روشهای مختلف که می‌توان به نگاه کردن کلمه عبور توسط فرد شیاد به هنگام عملیات برداشت توسط دارنده کارت و سپس سرقت کارت منجمله کیف زنی اشاره نمود.
- Skimming: دسترسی به اطلاعات از طریق پذیرنده‌های کارت و یا ارائه کارت به فرد دیگر که با تجهیزاتی امکان جعل آن را داشته باشد. در این حال مشتری اصل کارت را بهمراه خود داشته ولی تراکنشهائی ناخواسته توسط فردی دیگر در صورتحساب فرد مشاهده می‌شود.
- سوء استفاده برخی از کارکنان بانکها و آشنا به سیستم بدلیل ضعف در سیستم امنیتی دسترسی به اطلاعات مشتریان.

از عمده دلایل سوءاستفاده از کارتهای بانکی ایران و حسابهای مشتریان در سیستم یکپارچه را می‌توان به موارد کلی زیر اشاره نمود:

- عدم استفاده از شاخص‌های بیومتریک در کانالهای توزیع دیجیتالی.
- جعل کارت (Skimming) ناشی از بازیابی اطلاعات موجود در نوار مغناطیسی کارتهای بدهی بدلیل عواملی چون پایین بودن سطح امنیتی کارتها و عدم رمزنگاری اطلاعات، عدم استفاده از فناوریهای روز امنیتی کارتها مانند احراز هویت دوعاملی[۵۳] (TFA) در کارتها.

---

[51] Work Flow Management (WFM)

[۵۲] جهت اطلاع بیشتر مراجعه شود به: بیدآباد، بیژن و محمود الهیاری فرد فناوری اطلاعات و ارتباطات در تحقق سازوکار مشارکت در سود و زیان (بانکداری اسلامی)"، فصلنامه علمی- پژوهشی اقتصاد و تجارت نوین معاونت برنامه‌ریزی و امور اقتصادی وزارت بازرگانی، شماره سوم.

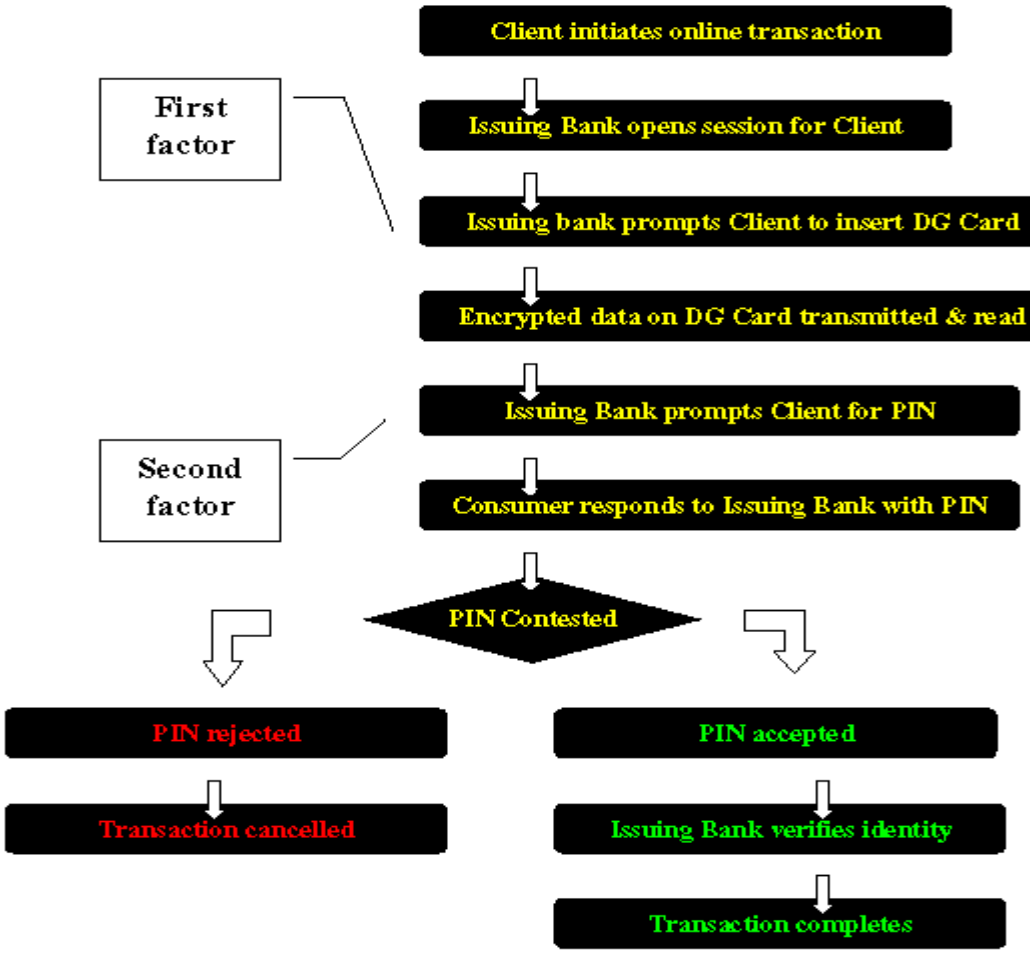
[۵۳] TWO Factor Authentication (TFA): بدلیل افشا شدن نام کاربر و کلمه عبور مشتریان و همچنین جعل هویت و افزایش ریسک عملیاتی ناشی جعل هویت و سایر ریسکها مانند Skimming و Fishing در اوائل اکتبر ۲۰۰۵ شورای نظارتی بر موسسات مالی فدرال (Federal

- ضعف در سیستم امنیتی و حدود دسترسی به اطلاعات مشتریان و در اختیار گذاشتن کلمه عبور کارمندان ناظر و تائیدکننده تراکنش و اعتماد به کاربران سطوح پائین‌تر.
- عدم توان ردگیری تراکنشها بطور مکانیزه.

راهکارهای نوین مدیریت ریسک عملیاتی بانکداری الکترونیک ایران

با گسترش محصولات و خدمات بانکداری الکترونیک و نقل و انتقال وجوه از طریق کانالهای دیجیتالی اینترانتی و اینترنتی در ایران ضرورت ایجاد واحد ریسک عملیاتی در ادارات مدیریت ریسک در بانکهای ایرانی قوت گرفته است. بکارگیری فناوریهای نوین در خصوص حفاظت از اطلاعات محرمانه بانک و احراز هویت مشتریان در استراتژیهای بانکداری اینترنتی از جمله موارد تعیین کننده می‌باشد که در ذیل به آنها اشاره می‌شود و انتخاب هریک از راه‌حلها توسط بانکهای ایرانی بمنظور کاهش ریسک عملیاتی مورد تجزیه و تحلیل قرار خواهد گرفت. بطور کلی راهکارهای

Financial Institutions Examination Council) طی نامه‌ای از موسسات مالی و اعتباری تقاضا نمود که تا پایان سال ۲۰۰۶ روش احراز هویت دوعاملی (TFA) را اتخاذ نمایند. الگوریتم احراز هویت جهت انجام تراکنشها TFA بشرح ذیل می باشد:



جهت اطلاع بیشتر مراجعه شود به:

www.dg-card.com/DG%20Card_File/DG%20Card%20Online%20Banking%20Executive%20Summary.pdf

حفاظت از اطلاعات محرمانه و حیاتی بانک و احراز هویت مشتریان از طریق فناوریهای ذیل صورت می گیرد:

- کلمه شناسایی شخصی[۵۴] (PINs)
- گواهی دیجیتالی با استفاده از زیرساخت کلید عمومی[۵۵][۵۶](PKI-Enabling)
- تجهیزات فیزیکی و نرم‌افزاری از ابعاد مشتریان و بانک:
  - کارتهای هوشمند (مشتریان)
  - کلمه شناسایی یک رویه[۵۷] (OTPs) (مشتریان)
  - ورودیهای USB (مشتریان)
  - استفاده از[۵۸] TOKEN (مشتریان)

حال باتوجه به راهکارهای نوین جهت احراز هویت مشتریان و کاهش ریسک عملیاتی از طریق کانالهای از را دور دیجیتالی مانند بانکداری اینترنتی در جدول زیر بطور تطبیقی راهکارهای منتخب بانکهای ایرانی را نشان خواهیم داد.

---

[54]Personal Identification Number(PINs)

[۵۵] به فرآیند تجهیز برنامه های کاربردی به استفاده از زیرساخت کلید عمومی، تواناسازی برنامه‌ی کاربردی به کلید عمومی گفته می‌شود. به واسطه این تغییر، نرمافزارها قادر خواهند بود سرویس‌های چهارگانه احراز هویت، محرمانگی، جامعیت و عدم انکار را مورد استفاده قراردهند.

[56]Public Key Infrastructure(PKI)

[57] One-Time Passwords

[۵۸] Token: یک نوع تجهیزات سخت‌افزاری است که ممکن است بعنوان بخشی از احراز هویت چند منظوره(Multifactor Authentication) تلقی شود.بطور کلی سه نوع Token وجود دارد که بشرح ذیل می‌باشد :

- تجهیزات یواس بی توکن(USB Token Device): این نوع از توکن بعنوان یکی از قطعات رایانه‌ای بسیار کوچکی است که به درگاه یو.اس.بی رایانه متصل می‌شود و بعنوان شرط لازم جهت ورود به سیستم و حساب بانک اینترنتی محسوب خواهد شد. احراز هویت سخت‌افزاری بهمراه ورود کلمه عبور مانع از دسترسی افراد غیر مجاز به اطلاعات محرمانه از جمله حساب مشتریان خواهد بود.
- کارت هوشمند (Smart card): این نوع از توکن شبیه بک کارتهای اعتباری می‌باشند. این کارت داری یک پردازشگر کوچکی است که اطلاعات را پردازش و ذخیره می‌نماید. حساسیت این کارت به دستکاری نمودن آن و غیر قابل کپی برداری آن از جمله عواملی است که موجب تقویت امنیت در احراز هویت خواهد شد. اصلیت کارت بعنوان فاکتور اول و ورود کلمه عبور بعنوان فاکتوردوم در این توکن بشمار می‌آید.بکارگیری این نوع توکن مستلزم وجود تجهیزات جانبی کارت خوان که متصل به رایانه مشتری باشد به همراه راه اندازهای نرم‌افزاری و سخت‌افزاری است که شاید بعنوان نقاط ضعف در بکارگیری این راهکار بشمار می‌رود.
- توکن ایجادکننده کلمه عبور(Password- Generating Token): این نوع از توکن ایجادکننده کلمه عبور منحصر بفرد می باشند و بغنوان OTPs شناخته می‌شوند.و هر بار توکن کلمه عبور مختلفی را تولید می‌نماید. مشتریان در مرحله اول نام و کلمه عبور معمولی خود را وارد می‌نمایند(فاکتور اول احراز هویت) و در مرحله دوم توکن کلمه عبور بعدی را ایجادمیکند (فاکتور دوم احراز هویت). مشتریان در درجه اول از طریق کلمه عبور معمولی و در درجه دوم انطباق کلمه عبور ایجاد شده توسط توکن با سرویس دهنده احراز هویت می‌شوند.

جدول۵: راهکارهای امنیتی احراز هویت مشتریان و امنیت شبکه بانکهای ایرانی

شرح	احراز هویت یک فاکتور (کلمه عبور)	استفاده از OTPs، از طریق تلفن همراه و E-mail	یو.اس.بی. توکن	کارت هوشمند	توکن ایجاد کننده کلمه عبور	امضای دیجیتالی	شاخص بیومتریک	CSIRT SOC NS
بانک مرکزی	–	–	–	–	–	–	–	√
ملی	√	–	–	√	√	√	–	√
صادرات	√	–	–	√	√	√	–	√
ملت	√	–	–	√	√	√	–	√
سپه	√	√	–	√	√	√	–	√
تجارت	√	–	–	√	√	√	–	√
رفاه	√	–	–	√	√	√	–	√
توسعه صادرات	√	√	–	√	√	√	–	√
کشاورزی	√	√	–	√	√	√	–	√
مسکن	√	√	–	√	√	√	–	√
صنعت ومعدن	√	√	–	√	√	√	–	√
پارسیان	√	√	–	√	√	√	–	√
کارآفرین	√	√	–	√	√	√	–	√
سامان	√	–	–	√	√	√	–	√
پاسارگاد	√	–	–	√	√	√	–	√
سرمایه	√	–	–	√	√	√	–	√

نتیجه‌گیری و توصیه سیاستی

بانکها بعنوان یکی از بنگاه‌های واسطه‌گر مالی در دو بازار مالی فعالیت می‌نمایند بطوریکه از سوئی بعنوان تقاضاکننده و از سوئی دیگر بعنوان عرضه‌کننده منابع پولی بشمار میروند. از اینرو ماهیت و ساختار این نوع کسب‌وکار توام با ریسک می‌باشد که برای رسیدن به اهداف استراتژیک در منظرهای مختلف در نقشه استراژی می‌بایست واحدی تحت عنوان واحد ریسک بمنظور شناسائی، سنجش و مدیریت ریسک ایجاد شود. ریسکهای مورد نظر از سوی واحد مدیریت ریسک بیشتر شامل ریسکهای سیستماتیک است به نحوی که بتوان با سازوکارهائی آنها را شناسائی، سنجش و همچنین مدیریت نمود. یکی از ریسکهایی که با ورود فناوری اطلاعات در حوزه کسب و کارها و بخصوص موسسات مالی، ظهور یافته ریسک عملیاتی داری الکترونیک می‌باشدکه با اجرایی شدن داری الکترونیک بیشترین دغدغه را برای دارن فراهم نموده است. شاید نگرانی ناشی از ریسک عملیاتی بیشتر مربوط به شیادیها و تقلبهائی است که در محیط سایبر بوجود می‌آید. حال آنکه بر اساس آمارهای منتشر شده معتبر جهانی این بخش از ریسکها و ضرر و زیانهای مربوط

به آن سهم کمی از مجموع ضرر و زیانها و ریسکهائی است که در محیط سایبر ایجاد می‌شوند، و دارن کمتر به این موضوع توجه می‌نمایند. انواع تقلبها و شیادیها در داری الکترونیک که ناشی از جعل عنوان، سرقت اطلاعات مشتریان و کاربران در قالبهای Phishing و Skimming ظهور می‌نماید، بخش کوچکی از وظائف مدیریت ریسک را شامل می‌شود. از اینرو، ریسکهای درون سیستمی ناشی از انواع اختلال در سیستمهای یکپارچه، و ریسکهای برون سیستمی دیگر مانند دزدیده شدن انواع کارتها، نفوذ به سیستمهای اطلاعاتی که ممکن است هزینه سربار ها را چندین برابر بیشتر از ضرر و زیانهای ناشی از کلاهبرداریها در محیط سایبر مانند Phishing و Skimming را موجب می‌شوند بایست مورد توجه مدیریت ریسک قرار گیرد.

در این بررسی برای نمونه انواع خطاها از نوع ریسک عملیاتی درون سیستمی دستگاههای خودپرداز ملی ایران بر اساس آمارهای سال ۹۲ شناسائی و آنگاه میزان ضرر و زیانها و یا بعبارت دیگر هزینه فرصت ناشی از ظهور این خطاها بر اساس قیمتهای سال ۹۲ محاسبه و برآورد شد. بر این اساس بطور متوسط هر دستگاه خودپرداز در ملی ایران ۴۵ روز را بدلایل انواع خطاها از به قطع ارتباط مخابراتی، قسمت پرداخت، چاپگر مشتری، چاپگر ژورنال، سوپروایزر و همچنین کارتخوان متوقف و فاقد توان لازم در ارائه خدمات به مشتریان می‌باشد. هزینه سربار ناشی از انواع خطاهای مورد بررسی برای دستگاه‌های خودپرداز این به قیمتهای سال ۹۲ برابر با ۱۱۳۱ میلیارد ریال برآورد می‌شود. ایجاد واحد هشدار امنیت داده ها و کارشناسی ریسک عملیاتی در ادارات مدیریت ریسک، ارتقاء فناوریهای امنیتی کارتها، استقرار Core banking کامل و مدیریت گردش کار (WFM) جهت ردگیری تراکنشها و رفع مغایرتها عمده راهکارهائی است که بمنظور کاهش ریسک عملیاتی دستگاه‌های خودپرداز و همچنین کارتها پیشنهاد می‌شود.

منابع

بیدآباد، بیژن و محمود الهیاری فرد، "مدیریت ریسک عملیاتی دستگاه های خودپرداز"، ۱۳۸۴
http://allahyarifard.ir/Papers/risk_management_in_e_banking.pdf

الهیاری فرد، محمود (۱۳۸۴)، خدمات داری الکترونیک و نیازهای اجرائی آن در مقایسه تطبیقی هزینه عملیاتی خدمات مختلف ی، پژوهشکده پولی ویانکی، مرکزی ایران
http://www.markazeketab.com/bookview.aspx?bookid=1212117.

بیدآباد، بیژن، محمود الهیاری‌فرد، "بهای تمام شده خدمات داری الکترونیک ملی ایران"،مجموع مقالات سخنرانیهای سومین کنفرانس بین‌المللی تجارت الکترونیک وزارت بازرگانی، تهران ، ۱۳۸۴.
http://allahyarifard.ir/Papers/baha-bank-1383.pdf

الهیاری‌فرد، محمود، "خدمات بانکداری الکترونیک"، مجموعه سخنرانیهای پانزدهمین کنفرانس سیاستهای پولی و ارزی، پژوهشکده پولی و ی مرکزی ایران ۱۳۸۴.

http://allahyarifard.ir/Papers/baha-bank-1381.pdf
www.srccyber.com/pdf/CyberLLC-01-risk-mgmt-soc_05.pdf
www.highstreetit.com/images/uploads/HIGHSTREET_NOC_final_0.pdf
www.bis.org/publ/bcbs98.pdf