تهدیدات امنیتی در سیستم‌های اطلاعاتی حسابداری رایانه‌ای

دکترمحمد عرب‌مازاریزدی
دانشیار دانشگاه شهیدبهشتی
نازنین محمدی‌استخری
دانشجوی کارشناسی ارشد حسابداری

تغییرات سریع در فناوری اطلاعات، گسترش همه جانبه سیستم‌های کاربرپسند[1] و تمایل عظیم سازمان‌ها در تهیه و اجرای سیستم‌ها و نرم‌افزارهای جدید و روزآمد، سبب شده تا رایانه‌ها خیلی آسان‌تر و وسیع‌تر از گذشته مورد استفاده قرار گیرند و وظایف حسابداری در مقایسه با گذشته سریع‌تر و با دقت بیشتری انجام شوند. از طرف دیگر، این فناوری پیشرفته، خطرات تازه و البته مهمی را در مورد نحوه تامین امنیت و اطمینان از صحت و درستی اطلاعات حاصل از سیستم‌های **اطلاعاتی حسابداری رایانه‌ای**[2] ایجاد کرده است. در بیشتر موارد، فناوری نوین اطلاعات بسیار سریع‌تر از فناوری‌های کنترلی، پیشرفت کرده و توسعه می‌یابد. از طرفی، این پیشرفت‌ها به هیچ روی با پیشرفت مهارت‌ها و آگاهی‌های کارکنان همسان نیست. در این مقاله، نظری اجمالی بر تهدیدات امنیتی سیستم‌های اطلاعاتی حسابداری رایانه‌ای خواهیم داشت، طبقه‌بندی‌های گوناگون تهدیدات امنیتی بیان خواهد شد و دلایل این تخلفات به شکل مختصر و خلاصه مشخص می‌گردد. در پایان، رویکردها و روش‌های سوءاستفاده امنیتی در این سیستم‌ها به همراه جزئیات، مورد بحث قرار خواهد گرفت.

پارکر بر طبق یک قانون قدیمی معتقد است که اگر چیزی را با یک چکش مناسب و بزرگ بکوبیم مسلماً خواهد شکست. در مورد رایانه‌ها، برنامه‌های رایانه‌ای، کاربران و داده‌ها، نیازی نیست که این چکش خیلی هم بزرگ باشد چون همه این اجزا شکننده و آسیب‌پذیرند و خیلی زود صدمه می‌بینند.(Parker, 1983) علاوه بر این به دلیل ظرفیت‌های بالای فرآیندها، تمرکز عظیم داده‌ها و سرعت زیاد عملیات در رایانه‌ها، راه‌های بسیاری برای صدمه زدن به سیستم رایانه‌ای وجود دارد. احتمال وارد شدن این صدمات به دلیل فاصله‌های زیاد جغرافیایی و استفاده از ظرفیت‌های ارتباطی داده‌ها که رایانه‌ها را در شبکه به هم متصل می‌کند، بیش از پیش افزایش یافته است.

دیویس معتقد است که امروزه تغییرات فناوری اطلاعات با دامنه بزرگ‌تری در مقایسه با گذشته صورت می‌گیرد و بسیاری از این تغییرات با سیستم‌های اطلاعاتی حسابداری سازمان‌ها مطابقت یافته‌اند. در کنار این سازگاری و تطبیق، پیشرفت‌های فناوری، تهدیدات امنیتی جدیدی را نیز برای سیستم‌های اطلاعاتی رایانه‌ای ایجاد

کرده‌است. (Davis, 1997) **شوایتزر** اصلی‌ترین تهدیدات امنیتی برای اطلاعات الکترونیک را به شرح زیر عنوان می‌کند:

- کاهش میزان پوشیدگی اطلاعات و خطر افشای اطلاعات محرمانه
- ربودن اطلاعات
- استفاده غیرمجاز از اطلاعات
- استفاده کلاه‌بردارانه از رایانه‌ها و تجهیزات
- کاهش صحت و درستی اطلاعات به علت تغییر یا دستکاری عمدی و غیرمجاز در داده‌ها
- کاهش خدمات رایانه‌ای به دلیل اعمال معاندانه عمدی و غیرمجاز (Schweitzer, 1987)

هوژن و سلین(Haugen, Selin, 1999) نیز عادی‌ترین نوع تقلب‌های رایانه‌ای را در شش طبقه به شرح زیر طبقه‌بندی کردند:

I. **تغییر داده‌های ورودی**: تغییر داده‌های ورودی نیازی به داشتن مهارت‌های رایانه‌ای چندانی ندارد. فقط لازم است بداند که سیستم چگونه عمل می‌کند تا بتواند ردپای خود را از بین ببرد.

II. **دزدیدن زمان و وقت رایانه**: استفاده از رایانه برای انجام دادن کارهای غیرمجاز، مثل انجام امور شخصی و ... تقلب محسوب می‌شود، حتی اگر فرد آگاه نباشد که در حال انجام عملی نادرست است.

III. **سرقت نرم افزار**: تخمین زده می‌شود که در ازای هر نسخه کپی قانونی از یک نرم‌افزار، بین ۱ تا ۵ مورد کپی‌برداری غیرقانونی از آن نرم‌افزار صورت می‌گیرد و این عمل برای صنعت نرم‌افزار، هزینه‌ای بین ۲ تا ۴ میلیارد دلار در سال خواهد داشت.

IV. **تغییر یا ربودن پرونده‌های داده‌ها**: اطلاعات ممکن است اغلب از سوی کارکنان ناراضی برای صدمه زدن به سازمان و ایجاد آثار زیان‌بار تغییر یابند، حذف شوند و یا مورد دستکاری قرار گیرند. همچنین ممکن است که اطلاعات به سرقت رفته و به رقبا یا سایر کسانی فروخته شوند که بتوانند از آن اطلاعات منفعت و فایده‌ای کسب کنند.

V. **دزدی یا استفاده نادرست از خروجی رایانه**: شبکه‌های رایانه‌ای در سازمان‌ها غالباً داده‌های خروجی از رایانه‌ها را در معرض دسترسی تعداد زیادی از کاربران قرار می‌دهند. به‌عنوان نمونه، از طریق چاپگرهای مشترکی صورت می‌گیرد که در مکان‌های عمومی سازمان برای دسترسی راحت‌تر همه افراد قرار داده می‌شوند. از طرفی صفحه نمایش رایانه غالباً به سهولت از سوی دیگران قابل مشاهده است و اطلاعات فرستاده شده از طریق ایمیل‌های داخل شرکت، ممکن است در قسمتی از سازمان متوقف شوند. هرچقدر اطلاعات خروجی‌های سیستم حساس‌تر باشند، به همان میزان توجه و کنترل مورد نیاز برای آن اطلاعات هم افزایش می‌یابد.

VI. **دسترسی غیرمجاز به سیستم یا شبکه**: با توسعه استفاده از اینترنت و انعطاف‌پذیری و آسانی که سیستم‌های شبکه‌ای پیدا کرده‌اند، لازم است که در مورد پرونده‌های حساس در سیستم مراقبت، توجه خاصی به عمل آید. شبکه‌ها نیز به دلیل ضعف امنیتی، غالباً از سوی حکرها آسیب‌پذیر هستند.

عوامل داخلی و خارجی بسیاری وجود دارد که سبب نقض امنیت سیستم می‌شود. بیشترین دلایل داخلی به کارکنان سازمان ارتباط پیدا می‌کند، یعنی کسانی که به دارایی‌ها و سیستم‌های حسابداری سازمان دسترسی دارند. مشکلات سازمانی و فنی داخلی از قبیل کنترل‌های ضعیف داخلی، خط مشی‌های ضعیف کارکنان و نبود صداقت و درستی در سطوح بالای سازمانی از عمده‌ترین دلایل تهدیدات امنیتی است. این موضوع می‌تواند شامل مواردی چون برنامه‌های پاداش ناکافی، قوانین انضباطی ضعیف و سهل‌انگارانه، گسترش خصومت و عداوت و سایر موارد تحریک‌آمیز دیگر نیز باشد. طبق نظر **هوژن و سلین** به دلایل زیادی ممکن است که کارکنان جرایم رایانه انجام دهند و اقدام به دزدی از کاری نمایند که انجام می‌دهند. عمومی‌ترین این دلایل می‌تواند انتقام و کینه‌جویی، بدهی شخصی زیاد و فشارآور و فقدان کنترل‌های داخلی باشد. امروزه تجارت کاری بسیار رقابتی است و کارکنان استرس و فشار زیادی را تحمل می‌کنند. در نتیجه ممکن است احساس کنند که بیش از توان از آنها کار خواسته می‌شود و کمتر از حد معمول دستمزد دریافت می‌کنند و مورد تقدیر و تشکر هم

واقع نمی‌شوند. حال اگر همزمان، با مسائل شخصی جدی و دشواری نیز دست به گریبان باشند، انگیزه آنها برای انجام تقلب خیلی بالا خواهد رفت.

اگر به این معادله، کنترل‌های ضعیف داخلی و فناوری در دسترس رایانه‌ای را اضافه کنیم، که در انجام جرم کمک‌کننده می‌باشد، آنگاه فرصت انجام تقلب جنبه واقعی و عینی پیدا خواهد کرد. (Haugen, Selin, 1999) گاهی اوقات ارزیابی میزان ریسک وقوع جرایم رایانه‌ای در سازمان کاری دشوار است، اما سازمان‌ها می‌توانند با استقرار سیستم و اعمال کنترل داخلی مناسب شامل رویه‌های استخدامی خوب و برنامه‌های آموزشی مناسب، در مقابل وقوع جرایم رایانه‌ای ایستادگی کرده و میزان زیان وارده را به حداقل ممکن برسانند.

فهرست زیر که برخی از علل و دلایل تخلفات را بیان می‌کند بر پایه مطالعات کارشناسان بسیاری در زمینه مسایل امنیتی سیستم‌های اطلاعاتی الکترونیکی تهیه شده است: (لازم به ذکر است که امکان اضافه شدن موارد دیگری به این فهرست نیز وجود دارد).

الف) **طراحی سیستم به صورت ناقص** به نحوی که توان فراهم ساختن کنترل‌های موثر را در طول چرخه عملیاتی سیستم ندارد. در سیستم‌های دستی، همواره وجود کنترل‌ها امری بدیهی تلقی می‌شود اما سیستم‌های رایانه‌ای در فراهم ساختن کنترل‌ها و رویه‌های مناسب جایگزین ممکن است دچار نقصان شوند. در بسیاری از موارد سیستم‌های کاربردی بدون توجه به ملاحظات امنیتی کافی، توسعه و گسترش پیدا می‌کنند.

ب) **اشتباهات برنامه‌ریزی** که ممکن است منجر به ایجاد حفره‌های نفوذ و رخنه در طول اجرای سیستم شوند و خطاهای برنامه (عمدی یا غیرعمدی) که می‌توانند سبب بروز فعالیت‌های کنترل نشده یا نادرست شود. این نکته را همواره باید به‌خاطر داشت که هیچ نرم‌افزار بدون اشتباهی وجود ندارد.

ج) **کنترل‌های ضعیف یا نامناسب در خصوص دسترسی منطقی به سیستم**، که ممکن است منجر به نفوذ و رخنه به سیستم شود. تا چند سال پیش از این، بیشتر سازندگان رایانه مسائل امنیتی سیستم را به منظور حفاظت از داده‌ها، به عنوان گزینه‌ای اضافی به خریداران پیشنهاد می‌کردند که باید مبلغی جدا از هزینه نرم‌افزار برای آن پرداخت شود. اما امروزه بیشتر سازندگان، امکانات امنیتی لازم جهت نرم‌افزار و سخت‌افزار را به عنوان پیش فرض در نظر می‌گیرند و آن را به عنوان جزء لازم و مکمل بسته نرم‌افزاری می‌فروشند.

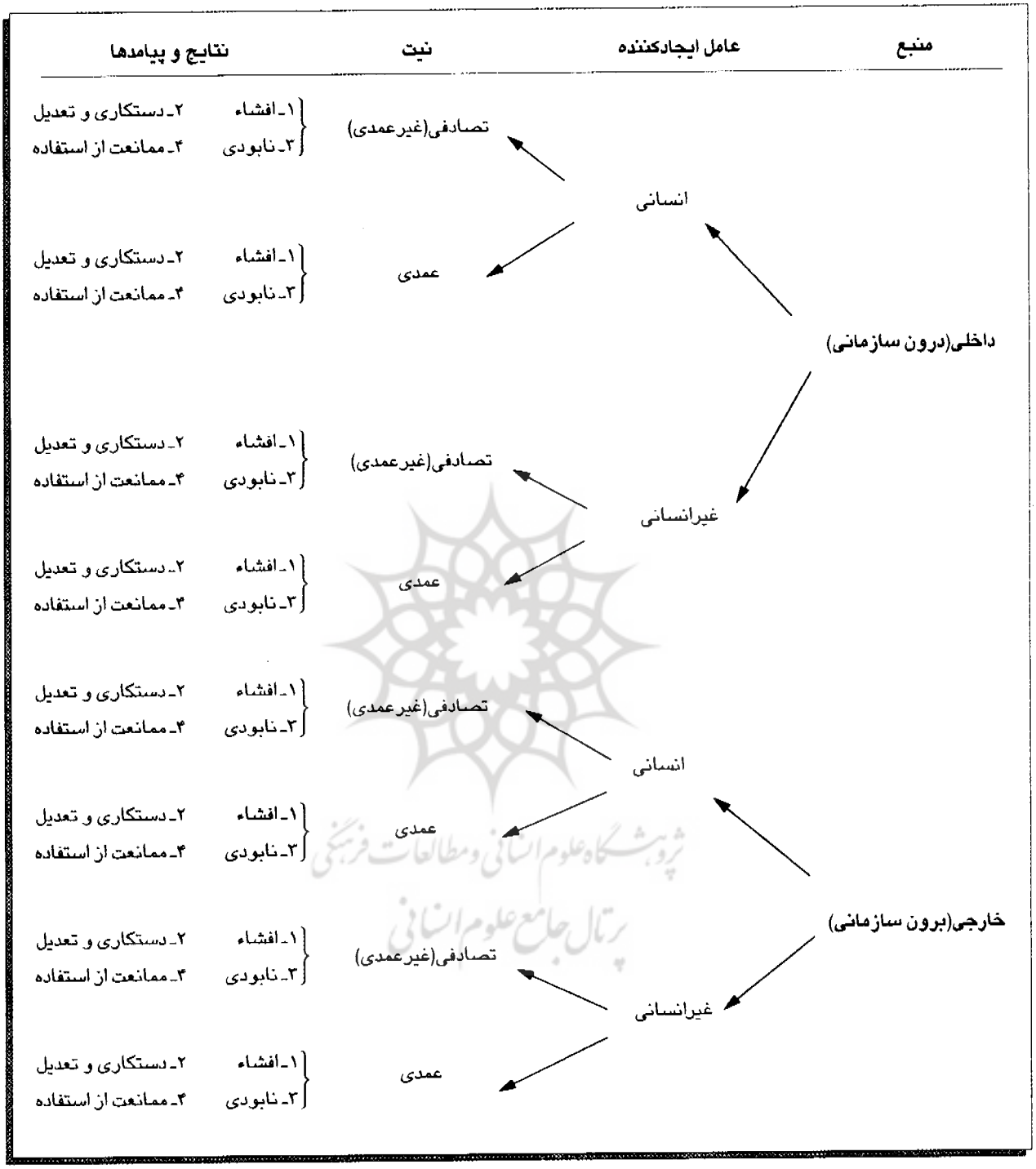
د) **کنترل غیرموثر مدیریت بر کارکنان**، که به افراد اجازه می‌دهد که در خارج از رویه خاص عملیاتی سیستم، عمل کنند یا اعمالی را انجام دهند که با بهترین خواسته‌های شرکت فاصله داشته باشد. تخلفات کوچک می‌توانند خیلی سریع رشد کرده و به تقلب‌های بزرگ منجر شوند.

همان گونه که بیان شد تهدیدات امنیتی سیستم‌های اطلاعاتی رایانه‌ای غالباً حاصل اعمال عمدی یا غیرعمدی است و ممکن است ناشی از منابع داخلی یا خارجی سازمان باشد. دامنه این تهدیدات می‌تواند از موارد خیلی بزرگ و تاثیرگذار تا رویدادهای جزیی و روزانه را در برگیرد. هنگام برنامه‌ریزی برای امنیت سیستم‌های اطلاعاتی رایانه‌ای لازم است تعداد دفعات وقوع و مدت هرکدام از این اعمال معین شود حتی اگر رویدادهایی کوچک و جزیی باشند. لازم به ذکر است که رویدادهای بزرگ و کوچک هر دو می‌توانند موجب بهم ریختگی در سیستم عملیاتی شوند و عملیات موثر سازمان را تضعیف کنند. در قسمت بعد، دیدگاه‌های گوناگونی ارائه شده است که در خصوص طبقه‌بندی تهدیدات امنیتی سیستم‌های اطلاعاتی حسابداری رایانه‌ای (CAIS) وجود دارد.

طبقه‌بندی تهدیدات امنیتی در سیستم‌های اطلاعاتی حسابداری رایانه‌ای (CAIS)

سیستم‌های اطلاعاتی حسابداری رایانه‌ای (CAIS) ممکن است از سوی دامنه گسترده‌ای از تهدیدات مانند تقلبات رایانه‌ای، اقدامات جاسوسی، خرابکاری، دشمنی، ویروس‌های رایانه‌ای، هکرها و سایر منابع خرابکاری مورد هدف قرار بگیرند. انتظار می‌رود که روز به روز تهدیدات امنیتی برای اطلاعات توسعه بیشتری یافته و ماهرانه‌تر و پیچیده‌تر شوند. تهدیدات امنیتی اطلاعات را می‌توان به **تهدیدات فعال**[3] و **تهدیدات انفعالی**[4] طبقه‌بندی کرد. تهدیدات انفعالی، رخدادهای غیرقابل پیش‌بینی طبیعی یا فیزیکی هستند و می‌توانند شامل خطاهای تصادفی انسانی

نمایشگر ۱ـ مدل چهاربعدی تهدیدات امنیتی سیستم‌های اطلاعاتی



(منبع: Loch et.al., 1992)

مانند آتش‌سوزی و سیل نیز باشند که کاملاً به صورت تصادفی اتفاق می‌افتند در حالی که تهدیدات فعال، معمولاً عمدی هستند و از روی عناد و دشمنی واقع می‌شوند. به‌طور بالقوه، این گروه از تهدیدات را می‌توان پیش‌بینی و از وقوع آنها جلوگیری کرد. این تهدیدات ممکن است توسط عوامل داخلی یا خارجی واقع شوند و در عین حال حاصل اعمال مستقیم یا غیر مستقیم باشند.

پارکر معتقد است که تهدیدات امنیتی را می‌توان بر طبق

نوع عمل آن تهدیدات به سه گروه طبقه‌بندی کرد: بلایای طبیعی، خطاها و غفلت‌ها، و اعمال عمدی. (Parker, 1983) دو گروه آخر هم ممکن است شامل بلایایی مثل آتش‌سوزی‌ها، سیل‌ها و انفجارها باشند که توسط افراد ایجاد شده‌اند. این نوع از اعمال را می‌توان به شکل ساده‌ای به دو گروه عمدی و غیرعمدی طبقه‌بندی کرد. بسیاری از اعمال عمدی از جمله تقلب، دزدی، اختلاس، اخاذی و شرارت اعمالی هستند که جزء جرایم طبقه‌بندی می‌شوند.

رینر و همکاران تهدیدات امنیتی سیستم‌های رایانه‌ای حسابداری را تحت سه گروه اصلی طبقه‌بندی کرده‌اند: تهدیدات فیزیکی، دسترسی‌های غیرمجاز و دسترسی‌های مجاز که ممکن است ناشی از منابع داخلی یا خارجی باشند. آنها معتقدند که اقدامات امنیتی برای دسته سوم که تهدیدات ناشی از دسترسی‌های مجاز می‌باشند دشوارترین نوع از اقدامات از جهت استقرار و برقراری کنترل‌های امنیتی می‌باشند.(Rainer et. al., 1991)

لاخ و همکاران در خصوص بحث امنیت سیستم‌های اطلاعاتی، مدلی چهاربعدی ارائه کردند. بر طبق این مدل، تهدیدات امنیتی ممکن است مثل تهدیدات ناشی از اعمال کارکنان یا عیب و نقص رویه عملکرد سازمان داخلی باشند یا اینکه مثل اعمال هکرها یا بلایای طبیعی خارجی باشند. براساس این مدل، بعد دیگر هر تهدید عامل ایجادکننده[5] می‌باشد، بعضی از تهدیدها ناشی از اعمال انسانی هستند حال آنکه برخی دیگر نتیجه رویدادهای طبیعی یا غیرانسانی می‌باشند. در نهایت اعمال، صرف‌نظر از منبع آن اعمال می‌توانند عمدی یا غیرعمدی باشند. (**نمایشگر ۱**) یک اپراتور رایانه که عمداً پرونده‌های حاوی اطلاعات مهم را از بین می‌برد، ممکن است در موقعیتی قرار داشته باشد که بتواند پرونده‌های پشتیبان این اطلاعات را نیز نابود سازد. (Loch et. al. 1992)

در ادامه این بحث، تهدیدات امنیتی سیستم‌های اطلاعاتی حسابداری رایانه‌ای (CAIS) برطبق منبع ایجاد آنها (داخلی در مقابل خارجی)، عامل ایجادکننده آن (انسانی در مقابل غیرانسانی)، قصد و نیت فرد مرتکب شونده (غیرعمدی در مقابل عمدی) و در نهایت زیان و خسارت وارده به سیستم (خرابکاری فیزیکی در مقابل خرابکاری منطقی) با جزییات بیشتری توضیح داده خواهند شد. تهدیدات امنیتی هر مرحله از سیستم اطلاعات حسابداری رایانه‌ای (CAIS) شامل ورودی، پردازش و خروجی نیز در قسمت جداگانه‌ای با جزییات بیشتری شرح داده خواهد شد.

همان‌گونه که قبلاً نیز گفته شد تهدیدات امنیتی را با توجه به منبع ایجاد آن تهدیدات می‌توان به دو گروه درون‌سازمانی (داخلی) و برون‌سازمانی (خارجی) طبقه‌بندی کرد. کارمندان سازمان به عنوان مهم‌ترین منبع تهدیدات امنیتی داخلی هستند، حال آنکه هکرها و بلایا و اتفاقات طبیعی به عنوان منبع عمده تهدیدات خارجی قرار می‌گیرند. برخی معتقدند که امروزه کارکنان درون سازمان به شکل بالقوه‌ای می‌توانند خطرناک‌ترین دشمنان سیستم باشند و عمده‌ترین ریسک در سیستم‌های امنیتی مربوط به این قسمت می‌باشد. نتایج تحقیق پژوهشی در سال ۱۹۹۲ توسط لاخ و همکاران نشان می دهد که ۶۳درصد پاسخ‌دهندگان از وجود تهدیدات امنیتی با منشاء درون سازمانی رنج می‌برند و اکثر این تهدیدات (تقریباً ۷۲درصد) ناشی از عامل انسانی می‌باشند. نتایج این مطالعه در **نمایشگر ۲** ارائه شده است. (Loch et. al. 1992) گرچه در اغلب موارد، اشتباهات و دسترسی‌های غیرمجاز به اطلاعات ریشه اصلی مشکلات امنیتی در سیستم است اما شواهد نشان می‌دهد که کارکنان سازمان در موارد اندکی سعی می‌کنند تا موارد امنیتی سیستم را در سازمان خود نقض کنند.

بیشتر دزدی‌های صورت گرفته در بانک‌ها، مثل بسیاری از تقلبات در سایر سازمان‌ها، توسط کارکنانی انجام می‌شود که به اطلاعات داخلی سازمان دسترسی دارند. به طور نمونه، در بانکی در ایالت کالیفرنیا، کارمندی با دسترسی به کد انتقال محرمانه بین بانکی توانسته بود رقم ۱۰میلیون دلار به حساب شخصی خودش در سوئیس منتقل کند. بانک‌ها سالانه هزینه قابل توجهی را به دلیل این تقلبات و تهدیدات صورت گرفته از سوی هکرها، متقبل می‌شوند در حالی که بسیاری از آنها به منظور حفظ شهرت و اعتبار خودشان از اعلام ارقام دقیق و واقعی خودداری می‌کنند.

نمایشگر ۲ـ نتایج مطالعه پژوهشی لاخ و همکاران در سال ۱۹۹۲ در خصوص تهدیدات امنیت سیستم‌های اطلاعاتی

تهدیدات درون‌سازمانی ۶۳درصد	ورود غیرعمدی داده‌های نادرست	۱۶/۵درصد		
	ورود عمدی‌داده‌های‌نادرست توسط کارکنان	۲/۲درصد		
	کنترل‌های فیزیکی ضعیف و غیرموثر	۹/۱درصد		
	حذف عمدی داده‌ها توسط کارکنان	۳/۵درصد		
	حذف غیرعمدی داده‌ها توسط کارکنان	۱۶درصد		
	دسترسی‌های غیرمجاز کارکنان	۵/۷درصد		
	کنترل غیرکافی بر تجهیزات سیستم	۵/۹درصد		
	کنترل ضعیف ورودی‌ها و خروجی‌ها	۴/۱درصد		
	جمع	**۶۳ درصد**		
تهدیدات برون سازمانی ۳۷درصد	دسترسی توسط رقبا	۱/۹درصد	بلایای طبیعی	۱۹/۸درصد
	دسترسی توسط حکرها	۷/۵درصد	ویروس‌های کامپیوتری	۷/۸درصد
	جمع	**۹/۴درصد**	**جمع**	**۲۷/۶درصد**

تهدیدات انسانی در مقابل تهدیدات غیرانسانی

از بعد عامل ایجادکننده تهدید، تهدیدات را می‌توان به دو گروه تهدیدات انسانی و تهدیدات غیرانسانی طبقه‌بندی کرد. تهدیدات امنیتی انسانی، تهدیداتی هستند که از اعمال انسان سرچشمه می‌گیرند. این تهدیدات می‌توانند (مثل خطاهای انسانی) تصادفی و غیرعمدی بوده و یا عمدی باشند. تنوع استفاده‌کنندگان از سیستم (کارمندان، مشاوران، مشتریان، رقبا و یا حتی جامعه) و سطوح مختلف آگاهی این استفاده‌کنندگان، مساله فراهم ساختن مسائل امنیتی برای سیستم را پیچیده کرده است.

دیسویس معتقد است فناوری جدید، ریسک مسائل امنیتی را در سیستم‌های اطلاعاتی حسابداری افزایش داده است. خطاهای انسانی می‌توانند در قالب خطاهای ناشی از غفلت و **سهل‌انگاری**،[6] و یا **جرائم**[7] واقع شوند. خطای نوع اول وقتی رخ می‌دهد که فردی در انجام عمل درست و صحیح ناتوان باشد. مثلاً یک نمونه از این خطاها، ناتوانی یک کاربر در تهیه پرونده‌های پشتیبان مناسب از پرونده‌های ضروری سیستم خود است. خطای نوع دوم وقتی واقع می‌شود که فردی عملی را اجراکند که نادرست است یا انجام آن ممنوع شده است. به عنوان نمونه‌ای از این نوع خطا می‌توان جابجا کردن ۲رقم در داده‌های ورودی توسط یک کاربر را ذکر کرد یا حذف پرونده مهمی که امکان بازگرداندن آن یا تهیه مجدد آن مقدور نباشد. از سوی دیگر تهدیدات امنیتی غیرانسانی عموماً به تهدیدات فنی از قبیل نقص فنی سیستم یا سخت‌افزار و یا مشکلات نرم‌افزاری سیستم مربوط می‌باشند. تهدیدات غیرانسانی همچنین ممکن است ناشی از بلایای طبیعی چون سیل، زلزله و یا حتی نوسان‌های برقی سیستم نیز باشد. تهدیدات فنی سیستم غالباً متعددند و حتی گاهی اوقات برخی از آنها به درستی شناخته شده نبوده و بطور پیوسته در حال تغییر می‌باشند. جالب است به این نکته توجه داشته باشیم که برخی از این تهدیدات فنی ممکن است با اعمال انسانی نیز در ارتباط باشند. برای مثال، وارد کردن یک ویروس به سیستم از طریق استفاده از نرم‌افزار آلوده.(Davis, 1997)

تهدیدات غیرعمدی(تصادفی) در مقابل تهدیدات عمدی

جنبه دیگری برای طبقه‌بندی تهدیدات امنیتی سیستم‌های اطلاعاتی حسابداری رایانه‌ای (CAIS)می‌تواند نیت و قصد فرد انجام‌دهنده آن عمل باشد. از این نظر تهدیدات را می‌توان به دو گروه عمدی و غیرعمدی طبقه‌بندی کرد. تهدیدات غیرعمدی آن گروه از تهدیدات هستند که از قصد و نیت کینه‌جویانه و بدخواهانه از قبیل

خطاهای انسانی یا برخی از تهدیدات طبیعی و فیزیکی سیستم نشات نگرفته‌اند. از طرف دیگر تهدیدات عمدی، تهدیداتی هستند که دارای قصد و نیت بدخواهانه مثل خرابکاری یا تقلبات رایانه‌ای. تهدیدات عمدی شامل استفاده نادرست از دسترسی‌های مجاز به سیستم و یا دسترسی‌های غیرمجاز به سیستم (هک کردن) با قصد و نیت ایجاد فتنه، خرابکاری، دشمنی، تقلب یا دزدی می‌باشد. **هوژن و سلین** معتقدند که اعمال غیرعمدی، اگرچه هزینه‌ای را بر سازمان تحمیل می‌کنند، لیکن قابل اصلاح کردن هستند و می‌توان از طریق آموزش و نظارت از وقوع آنها جلوگیری به عمل آورد. از طرف دیگر، اعمال عمدی عموماً منجر به جرائم رایانه‌ای می‌شوند و شامل نابود کردن اجزای سیستم، حذف کردن یا تغییر دادن رکوردها یا پرونده‌ها و ... به منظور از بین بردن اطلاعات یا تولید اطلاعات نادرست هستند.(Haugen, Selin, 1999)

تهدیدات امنیتی فیزیکی به تهدیداتی اشاره دارند که نتیجه آنها خسارت و زیان فیزیکی وارده به سیستم اطلاعاتی است. این خسارت‌ها می‌تواند شامل خسارات وارده به اجزا و قسمت‌های مجموعه اطلاعاتی باشد و یا خسارات وارده به ساختار و محیطی باشد که سیستم در آنجا مستقر است. این تهدیدات می‌توانند هم ناشی از وقایع و بلایای طبیعی باشند و هم ناشی از سوانح و وقایعی که در درون سیستم اطلاعاتی روی می‌دهند.

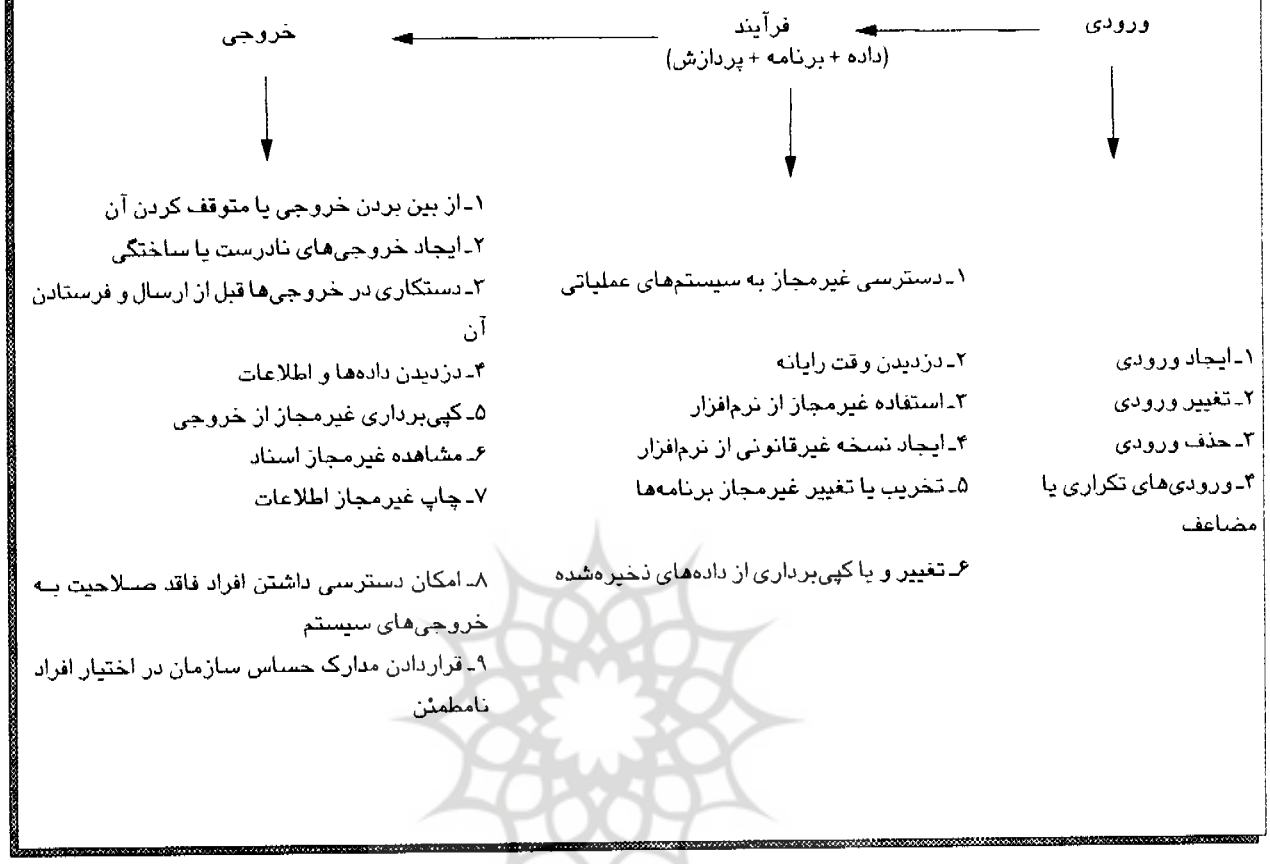
همان‌گونه که گفته شد تهدیدات فیزیکی سیستم‌های اطلاعاتی را عموماً در دو طبقه دسته‌بندی می‌کنند: وقایع محیطی و شرایط فیزیکی زیان بار برای اجزاء سیستم. وقایع محیطی شامل مواردی نظیر زمین لرزه، سیل، طوفان‌های الکتریکی، آتش‌سوزی باشد. شرایط فیزیکی زیان‌بار شامل مواردی از قبیل نقص معیارهای فیزیکی امنیتی سیستم، مشکلات سیستم برق‌رسانی، تهویه نامطلوب محیط، نفوذ آب به محیط و اتاق نگهداری رایانه‌ها و حتی گرد و غبار فضای اتاقهاست. بر طبق نظر **پارکر** عمده‌ترین تهدیدات برای نرم‌افزارها و دیسک‌های رایانه‌ای، تهدیدات فیزیکی هستند. شکسته شدن، ذوب شدن، خرد شدن، قرار گرفتن در میدان مغناطیسی و ... همه جزء اتفاقاتی هستند که می‌توانند نرم‌افزار را خراب کرده و اطلاعات ذخیره‌شده در آن را از بین ببرند. (Parker,1983)

تهدیدات امنیتی منطقی در سیستم‌های رایانه‌ای شامل خسارات منطقی وارده به نرم‌افزارها، برنامه‌ها و داده‌های ذخیره شده بر روی سخت‌افزار و فلاپی دیسک‌ها است. دیسک‌ها معمولاً دارای برچسب‌هایی هستند که بر روی دیسک چسبانده می‌شوند و در روی آنها محتویات دیسک و مطالب ذخیره شده در آنها نوشته می‌شود تا امکان شناسایی دیسک‌ها از یکدیگر وجود داشته باشد. در مراکز رایانه‌ای پیشرفته وسیله تشخیص دیسک‌ها شماره سریالی است که بر روی آنها چسبانده می‌شود. گرچه از بین بردن یا مخدوش کردن این برچسب‌ها، هزینه زیادی را بر سازمان تحمیل می‌کند زیرا بازیابی تک تک این دیسک‌ها و نصب برچسب مناسب بر هرکدام کاری وقت‌گیر و پر هزینه است. لیکن مساله این است که تهدیدات منطقی برای سیستم‌ها غالباً بسیار زیرکانه‌تر و ظریف‌تر از چنین مواردی است و می‌تواند منجر به هزینه‌ها و زیان‌های بسیار بیشتری در سازمان شود. برنامه‌های مختلف رایانه‌ای، یکی از اجزای مهم سیستم‌های اطلاعاتی است و به‌طور بالقوه یکی از زمینه‌های اصلی و عمده برای تهدیدات امنیتی محسوب می‌شود. وقتی برنامه رایانه‌ای در درون سیستم به ویروس یا سایر برنامه‌های مخرب آلوده شود ممکن است فهرست دسترسی‌های مجاز یا داده‌های موجود در سیستم را تغییر داده یا کلاً از بین ببرد. از طرفی، یک چنین برنامه‌ای می‌تواند در ارتباط با سایر قسمت‌ها و اجزای سیستم ایجاد اختلال کرده و عملکرد سایر اجزای را نیز مختل کند.

سه نوع عمده از تقلبات رایانه‌ای وجود دارد که عبارتند از:

- تهدیدات مربوط به داده‌های ورودی سیستم (شامل دستکاری در داده‌های ورودی سیستم)
- تهدیدات مربوط به فرآیند پردازش سیستم (شامل تغییرات غیرمجاز در عملیاتی که پردازش اطلاعات را انجام می‌دهد.)

نمایشگر ۳ـ انواع تهدیدات در مورد اجزای سه‌گانه سیستم



ـ تهدیدات مربوط به خروجی‌های سیستم (شامل دستکاری در این خروجی‌های و یا جلوگیری از ارائه آنها)

این تقسیم‌بندی در **نمایشگر ۳** نشان داده شده است.

یکی از معمول‌ترین راه‌های سوء استفاده امنیتی در سیستم‌های اطلاعاتی حسابداری رایانه‌ای (CAIS) تغییر ورودی‌های رایانه می‌باشد. از بین تقلبات رایانه‌ای، این نوع تقلب یکی از ساده‌ترین راه‌ها است زیرا به مهارت خاص و دانش ویژه‌ای از علوم رایانه‌ای نیاز ندارد. بنابراین لازم است که کنترل‌های مناسبی در قسمت‌های ورودی سیستم وجود داشته باشد تا بتواند از تغییرات و حذف و اضافات غیرمجاز در داده‌های ورودی به سیستم جلوگیری بکند. همان‌گونه که در نمایشگر ۳ نشان داده شد تقلبات مربوط به ورودی ممکن است شامل موارد زیر باشد:

این حالت شامل ایجاد داده در شکل و قالب عادی داده‌های ورودی سیستم می‌باشد. مثلاً درخواست هزینه غیرواقعی در بین سایر درخواست‌های هزینه، نمونه‌ای از این مورد است. در مواردی که نسخه‌ای هم از سفارش‌های ورودی به شکل عادی نگهداری نشود مثلاً در سیستم‌های مدرن امروزی انجام این کار راحت‌تر خواهد بود، زیرا که ورود داده‌ها و درخواست‌ها به شکل online صورت می‌گیرد.

تغییر و اصلاح داده‌های ورودی شامل ایجاد تغییراتی متقلبانه در داده‌های اولیه است، البته این تغییرات عموماً بر روی اقلامی صورت می‌گیرد که مورد تصویب واقع شده‌اند، لیکن هنوز وارد سیستم نشده‌اند. به عنوان مثال، افزایش یک

قلم هزینه، تغییر نام و آدرس مشتری یا تغییر نرخ بهره وام، نمونه‌هایی از این موارد هستند. در یک مثال واقعی، کارمندی توانسته بود نرخ بهره وام دریافتی توسط یکی از همکاران خود را از شرکت به هنگام ورود اطلاعات به رایانه کاهش دهد. در مقابل فرد وام‌گیرنده ماهانه ۵۰درصد مبلغ صرفه‌جویی شده در بهره وام را به عنوان پاداش به وی پرداخت می‌کرد.

حذف ورودی (Deletion of input)

این مورد شامل حذف داده‌ها قبل از وارد شدن آنها به سیستم می‌باشد و می‌تواند به شکل حذف یک قلم از اقلام یک دسته رکورد و یا حذف کل دسته به طور یک‌جا باشد. به عنوان نمونه، کارمند قسمت حقوق و دستمزد برگه‌های خاتمه خدمت کارکنان را از بین برده و اطلاعات را وارد سیستم نمی‌کرد و فقط اطلاعات حساب بانکی آن کارکنان را برای دریافت حقوق خود به حساب بانکی خاصی تغییر می‌داد که متعلق به خودش بود. این تقلب تا زمانی که وی برای مدتی بیمار شد و نتوانست در محل کار حاضر شود کشف نشده بود.

ورودی‌های مضاعف یا تکراری (Duplication of input)

این روش، از راه‌های آسان و موثر برای انجام تقلبات رایانه‌ای می‌باشد. روش کار بدین صورت است که از داده‌های اصلی و واقعی کپی تهیه می‌شود و آنگاه درخواست اولیه و کپی آن هر دو برای انجام سایر مراحل وارد سیستم می‌شوند.

تهدیدات امنیتی مربوط به پردازش سیستم

در این مرحله، فرد مجرم ممکن است دست به اقداماتی از قبیل تغییرات غیرمجاز در برنامه‌های رایانه‌ای و یا نرم‌افزارهای حسابداری بزند و یا اینکه به نابودکردن یا تغییر دادن داده‌های ذخیره شده در سیستم بپردازد و از این طریق، صدمات بزرگی را به سازمان و سیستم اطلاعاتی آن وارد بکند.

در ادامه به توضیح مختصری در خصوص اجزای اصلی مرحله پردازش داده‌ها یعنی پردازشگر، برنامه‌ها و دستورات رایانه‌ای و داده‌های ذخیره شده می‌پردازیم.

پردازشگر

یکی از بیشترین تقلب‌های رایانه‌ای و موارد نفوذ امنیتی به سیستم‌ها در مواقعی صورت می‌گیرد که از سیستم در انجام عملیاتی غیرمجاز استفاده شود. این مورد می‌تواند شامل دزدیدن زمان رایانه و سرویس‌های آن باشد. به‌عنوان مثال، کارکنان ممکن است از رایانه برای نگهداری از اطلاعات شخصی و یا انجام کارهای متفرقه خود استفاده کنند. حتی برخی از کارکنان ممکن است در طول ساعات کاری خود از سیستم‌های رایانه‌ای برای انجام بازی‌های رایانه‌ای نیز استفاده نمایند!

دستورات و برنامه‌های رایانه‌ای

با تغییر در عملکرد نرم‌افزاری مورد استفاده در عملیات سازمان نیز ممکن است تقلب رایانه‌ای صورت پذیرد. این عمل ممکن است شامل تغییر دادن نرم‌افزار، کپی‌برداری غیرقانونی از آن، استفاده از نرم‌افزار برای انجام فعالیت‌ها و اعمال غیرمجاز و آلوده کردن نرم‌افزار به ویروس‌های رایانه‌ای باشد. آنچه که مسلم است انجام این کارها برخلاف تقلبات مربوط به قسمت‌های ورودی و خروجی سیستم، نیازمند دانش خاص و مهارت‌های ویژه‌ای در علوم رایانه‌ای می‌باشد. بنابراین چنین تقلباتی کمتر از یک درصد از کل موارد تقلبات رایانه‌ای را تشکیل می‌دهد.

داده‌های ذخیره شده

سیستم اطلاعاتی رایانه‌ای ممکن است از طریق تغییر دادن یا از بین بردن پرونده‌های داده‌های سازمان یا کپی‌برداری و استفاده غیرمجاز از آن داده‌ها نیز صدمه ببیند. این نوع از تقلبات به مهارت رایانه‌ای کمتری در مقایسه با تقلبات مربوط به تغییر در نرم‌افزار نیاز دارد لیکن تنوع و حجم آنها از تقلبات مربوط به ورود داده‌ها بیشتر است. در یک مورد واقعی کارمندی با استفاده از یک آهنربای بسیار قوی توانسته بود به محتویات داده‌های دیسک‌های سازمان صدمه وارد کند. مساله مهم در این نوع تقلبات این است که در صورتی که این تغییرات در اطلاعات و داده‌ها کشف نشده باقی بمانند و وقوع جرم از سوی سازمان کشف نگردد، می‌توانند آثار زیان بارتری در مقایسه با حالت‌های دیگر در پی داشته باشد زیرا منجر به نتایجی نادرست و

گزارش‌هایی غلط می‌شوند.

آخرین راه برای نفوذ به سیستم اطلاعاتی رایانه‌ای و انجام تقلب، از طریق ربودن، استفاده نادرست، تغییر مسیر و یا نسخه‌برداری غیرمجاز از خروجی‌های سیستم است. خروجی سیستم‌ها معمولاً یا از طریق صفحه‌های نمایش و مانیتورها نشان داده می‌شوند و یا از طریق چاپگرها بر روی کاغذ چاپ شما می‌شوند. بنابراین افراد نزدیک صفحه نمایش رایانه به راحتی می‌توانند اطلاعات شما را مشاهده کنند، و یا در صورتی که افراد در سازمان دارای چاپگر مشترکی باشند، همواره امکان دارد که چشم‌های کنجکاوی باشند که سعی دارند به اطلاعات چاپ شده از طریق چاپگر دست پیدا کنند. همانند تقلبات مربوط به ورودی‌های رایانه، این نوع از تقلبات نیز نیاز چندانی به داشتن مهارت‌های رایانه‌ای ندارند.

علاوه بر تمام موارد پیشگفته، برخی موارد و نکته‌های دیگری نیز باید اشاره کرد که ممکن است جزیی باشند لیکن می‌توانند منجر به نتایج زیان‌باری برای سیستم اطلاعاتی مکانیزه شوند. برخی از این موارد عبارتند از:

- **در اختیار گذاشتن کلمه عبور رایانه** (password)، امروزه امری عادی بین کارمندان سازمان شده است در نتیجه فردی که کاربر یک رایانه خاص می‌باشد به تنهایی مسئول و پاسخگو در مورد کارها و فعالیت‌هایی نخواهد بود که ممکن است از طریق رایانه وی صورت گرفته باشد.
- ممکن است کارمندی به دلایلی از قبیل غیبت و یا بیماری همکاران خود برای انجام یک عمل فوری بتواند به سطوحی از دسترسی پیدا کند که بیشتر از حد مجاز تعیین شده برای وی می‌باشد. در این حالت هم پیدا کردن مسئول در قبال اعمال انجام شده کاری دشوار می‌باشد.

در این مقاله تهدیدات امنیتی فیزیکی و اطلاعاتی در سیستم‌های اطلاعاتی حسابداری رایانه‌ای (CAIS) مورد بحث و بررسی قرار گرفت. زیان‌های فیزیکی وارده ناشی از بلایا و اتفاقات طبیعی، از قبیل آتش‌سوزی و سیل، از جمله مواردی می‌باشند که می‌توانند خسارات عظیمی به سیستم اطلاعاتی وارد سازند. از سوی دیگر، قسمتی از تهدیدات سیستم اطلاعاتی ممکن است حاصل اعمال عمدی یا غیرعمدی انسانی باشد. منبع ایجاد تهدیدات برای سیستم ممکن است درون سازمانی (داخلی) باشد که ناشی از عملکرد کارکنان و مدیران سازمان است یا اینکه برون‌سازمانی (خارجی) باشد مثل تهدیدات هکرها و اتفاقات و سوانح طبیعی. در نهایت رویکردهای نفوذ امنیتی به سیستم از طریق سه مرحله عمده(ورودی، پردازش و خروجی) مورد بررسی قرار گرفت.

1- User- friendly

2- Computerized Accounting Information Systems (CAIS)

3- Active

4- Passive

5- Perpetrator

6- Ommision

7- Commision

1- Davis, Charles E. (1997), "An Assessment of Accounting Information Security", **The CPA Journal**, Vol. 67

2- Haugen Susan and J. Roger Selin (1999), "Identifying and Controlling Computer Crime and Employee Fraud", **Industrial Management and Data Systems**, Vol. 99.

3- Loch, Karen D., Houston H. Carr and Merrill E. Warkentin (1992), "Threats To Information Systems: Today's Reality. Yesterday's Understanding", **MIS Quarterly**, June.

4- Parker, Donn B. (1983), **Fighting Computer Crime**, Charles Scribner's Sons.

5- Rainer, Kelly Rex, Charles A. Snyder and Houston H. Carr (1991) "Risk Analysis For Information Technology", **Management Information Systems**, Vol. 8.

6- Schweitzer, James A. (1987), **Computers, Business, And Security**, Butterworth Publishers.