ارزیابی وضعیت مدیریت امنیت اطلاعات در مؤسسه‌های پژوهشی دولتی شهر تهران

زهرا خامدا

چکیده

گسترش روز افزون استفاده از فن‌آوری اطلاعات سبب شده است تا مقولهٔ امنیت اطلاعات به‌طور جدی مورد بحث و بررسی قرار گیرد. پیروی از استانداردی واحد در زمینهٔ مدیریت امنیت اطلاعات با تضمین جامع بودن، محرمانه بودن، و دسترس‌پذیر بودن اطلاعات امروزه ضرورتی شناخته شده است. بر این مبنا، هدف از پژوهش حاضر تعیین وضعیت مدیریت امنیت اطلاعات در مؤسسه‌های پژوهشی شهر تهران در مقایسه با شاخص‌های استاندارد بین‌المللی ایزو است. در این پژوهش از روش پیمایشی تحلیلی برای تجزیه و تحلیل داده‌ها استفاده شده است. جامعهٔ مورد مطالعه مؤسسه‌های پژوهشی دولتی شهر تهران، طبق آخرین فهرست منتشر شده توسط مرکز تحقیقات علمی کشور است. استاندارد به‌کار رفته، راهنمای عملی شمارهٔ ۱۷۷۹۹ سازمان جهانی استانداردسازی (ISO) است. بر این اساس پرسشنامه‌ای تنظیم شده و از مدیران مؤسسه‌های مذکور نظرسنجی به‌عمل آمده است. از بررسی یافته‌های پژوهش، با ۹۵ در صد اطمینان، می‌توان نتیجه گرفت که عملکرد مؤسسه‌های پژوهشی دولتی شهر تهران در زمینهٔ مدیریت امنیت اطلاعات بسیار ضعیف بوده است.

کلیدواژه‌ها: مدیریت. امنیت اطلاعات. اطلاع رسانی. مؤسسهٔ پژوهشی.

ارزیابی وضعیت مدیریت امنیت اطلاعات در مؤسسه‌های پژوهشی دولتی شهر تهران[1]

زهرا خامدا[2]

مقدمه

با رشد و توسعه روزافزون اطلاعات، یکی از مهم‌ترین دغدغه‌های ذهنی استفاده‌کنندگان اطلاعات امنیت آن است. خصوصاً اینکه امروزه با استفاده از اینترنت و توسعهٔ شبکه‌های محلی، مشکل نفوذ به رایانه‌ها و دسترسی به اطلاعات موجود شدت گرفته است.

هدف از ایمن‌سازی اطلاعات، تضمین "جامع بودن"، "محرمانه بودن"، و "دسترس‌پذیربودن" اطلاعات است.

وجود مدیریت و نظارت مؤثر از عوامل مهم کنترل‌های داخلی در یک سازمان به‌شمار می‌رود. مدیریت صحیح در یک سازمان موجب عملکرد صحیح تمام بخش‌های سازمان، از جمله واحد اطلاعات رایانه‌ای آن می‌شود. چنانچه مدیریت و نظارت درسازمان مناسب نباشد، اگرهم بهترین ضوابط کنترلی تدوین شده باشد، در اجرا ناموفق خواهد بود و قابل اعتماد نیست.

علاوه بر آن، لازمهٔ اثر بخش بودن مدیریت ایمنی، وجود آگاهی از مسائل ایمنی در تمام سطوح، مشخص بودن ضوابط ایمنی و پشتیبانی مدیران از موارد و ضوابط ایمنی

۱. برگرفته از: خامدا، زهرا (۱۳۸۲). "ارزیابی وضعیت مدیریت امنیت اطلاعات در مؤسسه‌های پژوهشی شهر تهران". پایان‌نامه کارشناسی ارشد، رشته علوم کتابداری و اطلاع‌رسانی، دانشکده روان‌شناسی و علوم تربیتی، دانشگاه تهران.

۲. کارشناس ارشد کتابداری و اطلاع‌رسانی دانشگاه تهران.

در سازمان است (آریا، ۱۳۸۰، ص ۹۳-۹۴).

تعیین اینکه چه کنترل‌هایی باید صورت گیرد نیاز به برنامه‌ریزی دقیق و توجه به جزئیات دارد. لذا ضروری است که هر سازمان نیازهای امنیتی خود را شناسایی کرده و سپس به انتخاب و اجرای کنترل‌های مربوط به آن بپردازد.

استاندارد "ISO/IEC 17799" در زمینهٔ مدیریت امنیت اطلاعات، با ارائه بعضی از راهکارها نقطهٔ آغازی برای پیاده‌سازی امنیت اطلاعات به‌شمار می‌رود.

بیان مسئله

بهره‌گیری از فن‌آوری نظام‌های اطلاعاتی برای افزایش کارآیی و بهره‌وری مناسب در اغلب زمینه‌ها به سرعت در حال گسترش است. استفاده از رایانه‌ها در مؤسسه‌های دولتی، صنایع، سازمان‌ها، و افراد حقیقی افزایش یافته است. تغییرات در فن‌آوری اطلاعات و افزایش تعداد کاربران و کاربران شبکه‌ها، طبیعت مسائل امنیتی رایانه‌ای را دگرگون ساخته است.

از سویی با اینکه پیشرفت‌های شگرفی در فن‌آوری رایانه حاصل شده است، در زمینهٔ آگاهی استفاده‌کنندگان از آسیب پذیری داده‌ها و اطلاعات و نیز مخاطرات مربوط به تغییرات غیر مجاز، افشا، و تخریب عمدی یا سهوی اطلاعات اقدام چندانی صورت نگرفته است.

به‌طور معمول (در اغلب نظام‌ها) مسئلهٔ امنیت تا قبل از مرحلهٔ تعریف نیازمندی‌های عملیاتی، به‌طور جدی مدّ نظر قرار نمی‌گیرد و نظام به‌طور مستقیم وارد مرحلهٔ پیاده‌سازی می‌شود. بدین ترتیب، دستیابی به یک سطح مناسب امنیتی برای سیستم در حال اجرا به ندرت امکان پذیر است. حتی در صورت عملی شدن چنین امنیتی، هزینه‌های ناشی از این امر در مقایسه با نظام‌هایی که از ابتدای طراحی، ملاحظات امنیتی را در نظر گرفته‌اند بسیار بالاتر خواهد بود (شیرازی، ۱۳۷۴، ص ۱۱۰).

در سال‌های اخیر در زمینهٔ ارزیابی امنیت، الگوهایی به منظور ایجاد استاندارد در جنبه‌های مختلف امنیت توسعه یافته است.

در این پژوهش سعی بر آن است که وضعیت مدیریت امنیت اطلاعات در مؤسسه‌های پژوهشی دولتی شهر تهران، در مقایسه با استاندارد "ISO /IEC 17799"، مورد ارزیابی قرار گیرد. در واقع، پژوهشگر می‌کوشد تا با بررسی شاخص‌های استاندارد

فوق، بدین سؤال اصلی پاسخ گوید که فرایند مدیریت امنیت اطلاعات در مؤسسه‌های پژوهشی دولتی شهرتهران تا چه اندازه با این استاندارد مطابقت دارد.

تعریف عملیاتی واژگان و مفاهیم پژوهش

مدیریت امنیت اطلاعات: مجموعه تمهیدات مدیریتی است که به منظور نیل به اصول امنیت اطلاعات به کار می‌رود.

امنیت اطلاعات: منظور دستیابی به اصول ذیل است:

الف. محرمانه بودن اطلاعات. اطمینان از اینکه اطلاعات فقط در دسترس اشخاصی است که مجوز دسترسی دارند؛

ب. *جامع بودن اطلاعات.* اطمینان از اینکه اطلاعات و روش‌های پردازش آن دقیق و کامل است؛

ج. *دسترس‌پذیربودن اطلاعات.* اطمینان از اینکه کاربران مجاز در هنگام نیاز، به اطلاعات دسترسی دارند؛

استاندارد ایزو. منظور راهنمای عملی شمارهٔ ۱۷۷۹۹ سازمان بین‌المللی استانداردسازی در زمینهٔ مدیریت امنیت اطلاعات است. این استاندارد ده شاخص اصلی دارد که هریک مورد آزمون قرار گرفته است.

پرسش‌های اساسی

پژوهش حاضر سعی دارد که به پرسش‌های ذیل پاسخ گوید:

۱. عملکرد مؤسسه‌های پژوهشی دولتی شهر تهران در زمینهٔ سیاست مدیریت امنیت اطلاعات چگونه است؟

۲. عملکرد مؤسسه‌های پژوهشی دولتی شهر تهران در زمینهٔ مدیریت امنیت سازمان چگونه است؟

۳. عملکرد مؤسسه‌های پژوهشی دولتی شهر تهران در زمینهٔ مدیریت امنیت اموال سازمان چگونه است؟

۴. عملکرد مؤسسه‌های پژوهشی دولتی شهر تهران در زمینهٔ مدیریت امنیت کارکنان چگونه است؟

۵. عملکرد مؤسسه‌های پژوهشی دولتی شهر تهران در زمینهٔ مدیریت امنیت فیزیکی و

محیطی سازمان چگونه است؟

۶. عملکرد مؤسسه‌های پژوهشی دولتی شهر تهران در زمینهٔ مدیریت امنیت ارتباطات و عملیات سازمان چگونه است؟

۷. عملکرد مؤسسه‌های پژوهشی دولتی شهر تهران در زمینهٔ مدیریت کنترل دسترسی به اطلاعات سازمان چگونه است؟

۸. عملکرد مؤسسه‌های پژوهشی دولتی شهر تهران در زمینهٔ مدیریت امنیت گسترش و نگهداری سیستم‌ها چگونه است ؟

۹. عملکرد مؤسسه‌های پژوهشی دولتی شهر تهران در زمینهٔ مدیریت تداوم عملیاتی سازمان چگونه است ؟

۱۰. عملکرد مؤسسه‌های پژوهشی دولتی شهر تهران در زمینهٔ مدیریت قوانین امنیتی وفنی سازمان چگونه است؟

هدف و فایده پژوهش

هدف از این پژوهش تعیین وضعیت مدیریت امنیت اطلاعات در مؤسسه‌های پژوهشی دولتی شهر تهران است. نتایج به‌دست آمده از این پژوهش شاید بتواند در سیاست‌گذاری و برنامه‌ریزی مدیریت امنیت اطلاعات در مؤسسه‌های پژوهشی دولتی شهر تهران مؤثر باشد.

امروزه ضرورت حفظ داده‌ها و سیستم‌ها به این دلیل قابل توجه است که ره‌آوردهای فن‌آوری معاصر عموماً در تصمیم‌گیری‌های مهم اتخاذ شده توسط حکومت‌ها و همچنین سازمان‌های معتبر جهانی نقش اساسی را ایفا می‌کنند. به‌علاوه، فن‌آوری پیشرفتهٔ صنعتی نیز مبتنی بر نظام‌های اطلاعاتی قابل اطمینان کارایی بهینه دارد. امروزه حجم قابل توجهی از مبادلات بازرگانی و مالی بین‌المللی با استفاده از فن‌آوری تبادل الکترونیکی داده‌ها انجام می‌شود. ایجاد کوچک‌ترین خللی در این نظام مبادلاتی، ضررهای هنگفتی را به طرفین مبادله تحمیل خواهد کرد که بعضاً ممکن است به ورشکستگی آنها بیانجامد.

براساس ارقام شورای عالی انفورماتیک ایران، میزان تجارت الکترونیکی در سال ۲۰۰۰، حدود ۴۰۰ میلیارد دلار و پیش بینی برای سال ۲۰۰۳، درحدود ۳۱۰۰ میلیارد دلار بوده است. در ایران هم بسیاری از شرکت‌ها، از شبکه‌های محلی

برای پردازش‌های کامپیوتری خود استفاده می‌کنند و تعدادی از شرکت‌ها و بانک‌ها هم فعالیت‌های تجاری را با استفاده از شبکهٔ گسترده انجام می‌دهند (آریا، ۱۳۸۰، ص ۴۵).

از سویی دیگر، در سال‌های اخیر، قوه قضاییهٔ کشور به بررسی پرونده‌هایی پرداخته است که از طریق نفوذ در سایت سازمان‌ها و ارگان‌ها اقدام به تخریب آنها کرده‌اند و یا قفل بسیاری از نرم افزارها راکه با صرف هزینه و انرژی زیاد تهیه شده شکسته‌اند. به‌طور مثال، می‌توان به ۱۸۷ مورد تعرض به سایت‌های مختلف در کشور اشاره کرد که خسارت مالی فراوانی به آنها وارد شده است (شهیدی، ۱۳۸۱، ص ۶).

شاید علت سرمایه‌گذاری اندک در بخش امنیت فن‌آوری اطلاعات این باشد که به آن صرفاً به منزلهٔ هزینهٔ نگریسته می‌شود و نه سرمایه‌گذاری؛ در حالی که براساس تجربهٔ جهانی لازم است که حدود ۳ـ۵ درصد از کل بودجهٔ فن‌آوری اطلاعات ـ و حتی تا حدود ۱۰ درصد از آن در بخش‌های پر خطر و حساس مثل خدمات مالی ـ صرف امنیت فن‌آوری اطلاعات گردد (دپارتمان صنعت و...، ۲۰۰۲، ص ۲).

به‌علاوه، اهمیت این پژوهش زمانی مشخص‌تر می‌شود که ماهیت و فلسفهٔ وجودی مؤسسه‌های پژوهشی مدنظر قرار گیرد. زیرا در این نوع مؤسسه‌ها:

۱. اطلاعات ذخیره شده ارزش فرهنگی، اجتماعی، ملی، و مانند آن دارد؛

۲. نتایج حاصل از پژوهش‌ها می‌تواند در سیاست‌گذاری‌های ملی مؤثر باشد؛

۳. امکان اتصال به اینترنت و شبکه‌های خارجی وجود دارد؛

۴. حس کنجکاوی و امکان تخریب داده‌ها زیاد است؛

۵. نظارت دقیقی بر استفاده از سیستم‌ها و شبکه وجود ندارد؛

۶. آگاهی افراد از مسائل امنیت اطلاعات محدود است.

فرضیهٔ پژوهش

عملکرد مؤسسه‌های پژوهشی دولتی شهر تهران در زمینهٔ مدیریت امنیت اطلاعات با استاندارد ایزو تفاوت دارد.

پیشینه

نظر به اهمیت موضوع پژوهش، علی‌رغم نو و بدیع بودن آن، تاکنون پژوهش‌های زیادی

خصوصاً از نظر فنی در داخل کشور صورت گرفته و توجه بسیاری از پژوهشگران به آن جلب شده است. اما آنچه این پژوهش را از سایر مطالعات انجام شده متمایز می‌سازد، رویکردی است که پژوهش حاضر به جنبه‌های مدیریتی امنیت اطلاعات دارد. به بیانی دیگر، مطالعات قبلی با حفظ ارزش ماهوی خود، جنبه‌هایی از امنیت اطلاعات را از نقطه نظر فنی و خاص از درون سیستم مطالعه کرده‌اند، حال آنکه این پژوهش با دیدگاهی مدیریتی و بیرون از سیستم به بررسی وضعیت کلیهٔ جنبه‌های امنیتی اطلاعات می‌پردازد. برخی پژوهش‌های انجام شده به صورت خلاصه بیان می‌شود:

روحانی (۱۳۷۲) در پایان‌نامهٔ کارشناسی ارشد خود با عنوان "طرح ایجاد شبکه‌های اطلاع‌رسانی در مراکز نظامی کشور" تأکید می‌دارد که آنچه در شبکه‌های محلی مورد توجه است امنیت اطلاعات است.

محضب (۱۳۷۳) در پایان‌نامهٔ کارشناسی ارشد خود با عنوان "ایمنی ارتباطات در شبکه‌های کامپیوتری" به مسئلهٔ امنیت شبکه که یکی از مهم‌ترین مسائل مطرح شده در مبحث شبکه‌های کامپیوتری است می‌پردازد.

نجفی (۱۳۷۳) در پایان‌نامهٔ کارشناسی ارشد خود به "رمز نگاری و مکانیزم‌های ایمنی در شبکه‌های کامپیوتری" می‌پردازد.

داود آبادی (۱۳۷۳) در پایان‌نامهٔ کارشناسی ارشد خود نیز در زمینهٔ "طراحی سیستم رمز نگاری RSA" تلاش کرده است.

عبدالهی ازگمی (۱۳۷۵) در پایان‌نامهٔ کارشناسی ارشد خود ضمن برشمردن اهمیت امنیت در شبکه، به "طراحی و پیاده‌سازی سرویس‌های امن برای شبکه‌های کامپیوتری" پرداخته است.

رجایی (۱۳۷۵) در پایان‌نامهٔ کارشناسی ارشد خود با اشاره با اینکه یکی از منابع اطلاعاتی گفتار انسان است و این که امروزه بحث مخفی کردن اطلاعات از دید اغیار اهمیت زیادی یافته است، در زمینهٔ "بررسی و تحلیل سیستم‌های رمزکننده آنالوگ صوت" پژوهش کرده است.

سلامت (۱۳۷۹) در پایان‌نامهٔ کارشناسی ارشد خود با مرور مفاهیم شبکه‌های کامپیوتری، بررسی مدل مرجع، شبکه اینترنت و بیان سیستم‌ها و مکانیزم‌های امنیتی، "امنیت شبکه‌های کامپیوتری" را تحلیل کرده است.

پور اسدی اورتاکندی (۱۳۷۹) در پایان‌نامهٔ کارشناسی ارشد خود با اشاره به افزایش

قابل توجه در مطالعه سیستم‌های الهام گرفته بیولوژیکی به "بررسی نقش سیستم‌های چند عامله به منظور مدیریت امنیت" پرداخته است.

رضوانی (۱۳۸۰) در پایان‌نامهٔ کارشناسی ارشد خود در مورد پیکر بندی و مدیریت حفاظ‌ها، "توصیف سطح بالای سیاست‌های امنیتی در حفاظ" را تهیه کرده است.

جاودانی (۱۳۸۰) در پایان‌نامهٔ کارشناسی ارشد خود با اشاره به اینکه امروزه سایت وب، به عنوان پرطرفدارترین سرویس شبکهٔ اینترنت، به سرعت در حال رشد و گسترش است "امنیت در سرورهای وب" را مورد بررسی و تحلیل قرار داده است.

و سرانجام بولوردی (۱۳۸۰) در پایان‌نامهٔ کارشناسی ارشد خود برای نخستین بار به طراحی "امنیت امضای دیجیتال کور گروهی آستانه" برای تضمین امنیت پیام پرداخته است.

در خارج از کشور نیز پژوهش‌هایی به‌صورت ذیل مشاهده می‌شود:

اس. اچ. فن سلمز[1] (۱۹۹۶) در مقاله خود با عنوان " امنیت اطلاعات در بزرگراه‌های الکترونیکی"، تعدادی از پروتکل‌های امنیتی اینترنت و شبکهٔ گسترده جهانی را مورد بررسی قرار می‌دهد.

برنارد[2] و روسو ون سلمز[3] (۱۹۹۸) در مقاله‌ای با عنوان "ارزیابی و گواهی امنیت اطلاعات در مقایسه با استاندارد "BS 7799" به تشریح و بیان ضرورت اجرای این استاندارد می‌پردازد.

روسو ون سلمز (۱۹۹۸) در مقالهٔ خود با عنوان "چرا امنیت اطلاعات مهم است؟"، اشاره می‌کند که امنیت اطلاعات دیگر موضوعی داخلی و محلی نیست، بلکه شرکای خارجی را نیز تحت تأثیر قرار می‌دهد؛ و تفسیر سطح بالایی از استاندارد TCSEC[4] (کتاب نارنجی)، و ضابطهٔ ITSEC (کتاب سفید) را ارائه می‌دهد.

استیسی[5] (۲۰۰۰) در گزارشی با عنوان "به‌سوی استانداردسازی امنیت اطلاعات: BS7799" راهنمای عملی استاندارد انگلیسی BS7799 را تشریح کرده و به بررسی وضعیت اجرای آن در میان شرکت‌های انگلیسی می‌پردازد. وی اظهار می‌دارد که فقط ۲۷ در صد از شرکت‌های انگلیسی دارای سیاست امنیت اطلاعات مشخصی هستند.

لونی[6] (۲۰۰۲) در پژوهشی با عنوان "تهدید امنیتی شما: کارمندان؟" بیش از یک سوم نقص‌های امنیتی نظام‌های رایانه‌ای در انگلیس را ناشی از کارمندان و یک سوم از

1. S. H. Von - Solms
2. Lynette Barnard
3. Rossouw Von-Solms
4 Trusted Computer Security Evaluation Criteria
5. Stacey
6. Loney

بدترین حوادث ایمنی را ناشی از ویروس‌های رایانه‌ای می‌داند.

ریزو[1] (۲۰۰۲) مدیر طرح پیمایشی "امنیت جهانی" با مطالعهٔ ۶۴۱ سازمان از بخش‌های دولتی سراسر جهان، به ارزیابی وضعیت امنیت اطلاعات پرداخته است. وی با بیان آماری برخی نتایج به‌دست آمده توصیه می‌کند که به منظور پیاده‌سازی یک ظرفیت امنیتی مؤثر، سازمان‌ها نیاز به تعیین ضعیف ترین نقاط اتصال خود دارند؛ و یک معماری وسیع امنیتی را جهت تحقق اهداف مدیریت امنیت ضروری می‌بینند.

هو[2] و موری[3] (۲۰۰۲) در مقالهٔ تحقیقی خود با عنوان "حفاظت از اموال اطلاعاتی در مؤسسات مالی: ایزو ۱۷۷۹۹"، مقایسهٔ نتایج مطالعه و نیز استناد به آخرین گزارش آماری CSI، اظهار می‌دارند که ۹۰ درصد از سازمان‌ها در سال ۲۰۰۱، حوادث امنیتی را تجربه کرده و ۸۰ درصد از شرکت‌ها می‌توانند خسارت‌های مالی ناشی از آن را محاسبه کنند. سپس با تبیین عملکرد مؤسسه‌های مالی بر لزوم اجرا و پیاده‌سازی استاندارد فوق در مؤسسه‌های مذکور تأکید می‌کنند.

دپارتمان صنعت و تجارت انگلیس[4] (۲۰۰۲) با همکاری چندین شرکت معتبر انگلیسی، در پژوهشی با عنوان "شکست‌های امنیت اطلاعات : پژوهش ۲۰۰۲" اذعان می‌دارد که اطلاعات رگ حیاتی تجارت امروز، پشتیبانی از عملیات به‌هنگام، و امکان تصمیم‌گیری‌های مؤثر است؛ و تأکید می‌کند که دسترسی به اطلاعات صحیح توسط اشخاص مجاز، جهت تداوم عملیات تجاری ضروری است و نیل به این دسترسی را در گرو درک خطرات مربوط و معیارهای مقابله با آن می‌داند. این پیمایش به‌منظور کمک به شرکت‌های انگلیسی جهت درک خطرات مزبور در رویارویی با امنیت اطلاعات صورت گرفته است. این پژوهش بر آن است که، اهمیت امنیت اطلاعات، از نظر اولویت‌های برنامه‌ریزی و سیاست‌گذاری، در سال گذشته بیشتر شده است و بسیاری از شرکت‌ها پیشرفت‌های چشمگیری در کنترل‌های امنیتی خود داشته اند. در مقابل، خطرات و تهدیدات نیز به‌طور قابل توجهی افزایش یافته است، به‌طوری که نیمی از شرکت‌های انگلیسی، حداقل یک حادثهٔ امنیتی مخرب پیش از انجام پیمایش داشته‌اند. این پژوهش با نظرسنجی از شرکت‌های بزرگ و کوچک انگلیسی به نتایج قابل توجهی دست یافته است و تأکید می‌کند که سرمایه‌گذاری در بحث امنیت اطلاعات در زمان پژوهش بسیار کم بوده است و نیاز مبرم و فوری به آن

1. Rizzo
2. Ho
3. Murray
4. Department of Trade & Industry (DTI)

احساس می‌شود.

روش پژوهش و گردآوری داده‌ها

این پژوهش با بررسی رابطهٔ متغیرها رویکردی توصیفی دارد و روش پژوهش پیمایشی ـ تحلیلی است. جامعهٔ مورد مطالعه مؤسسه‌های پژوهشی دولتی شهر تهران است، که تعداد آنها مطابق با آخرین فهرست منتشر شده توسط مرکز تحقیقات علمی کشور در مجموع ۱۳۱ مؤسسه بوده است (مهرابی، ۱۳۷۹، فهرست). از این تعداد، با استفاده از روش نمونه‌گیری تصادفی، نمونه‌ای همگن مشتمل بر ۳۵ مؤسسهٔ پژوهشی دولتی مستقر در شهر تهران انتخاب و پرسشنامه میان مدیران توزیع گردید.

تجزیه و تحلیل یافته‌ها

جهت آزمون فرضیه، در این پژوهش از روش‌های آمار استنباطی (آزمون مجذور خی) استفاده شده است.

از بخش اول پرسشنامه، یافته‌های توصیفی به صورت ذیل بدست آمده است که پاسخ‌دهندگان:

۱. ارزش اطلاعات و سطح محرمانگی آن را برای مؤسسه، متوسط تا زیاد ارزیابی کرده‌اند.

۲. میزان وقوع حوادث امنیتی را در مؤسسه، خیلی کم تا کم ارزیابی کرده‌اند.

۳. خسارت مالی ناشی از وقوع و ترمیم حوادث امنیتی را، خیلی کم تا کم ارزیابی کرده‌اند.

۴. میزان موفقیت خود را در کنترل حوادث امنیتی، متوسط تا زیاد ارزیابی کرده‌اند.

بخش دوم پرسشنامه مشتمل بر ۳۶ پرسش، منطبق بر ۳۶ مؤلفه از ده شاخص اصلی استاندارد "ایزو ۱۷۷۹۹" است که به ارزیابی عملکرد مؤسسه‌های پژوهشی در طیف بسیارخوب، خوب، متوسط، ضعیف، و بسیار ضعیف می‌پردازد.

برای آزمون فرضیه از درهمکرد شاخص‌های اول تا دهم استفاده شده است که اطلاعات آماری آن در جدول شمارهٔ ۱ آمده است:

جدول ۱. توزیع فراوانی عملکرد مؤسسه از دیدگاه مدیران

عملکرد مؤسسه	فراوانی مشاهده‌شده (Fo)	درصد فراوانی (درصد)	فراوانی مورد انتظار (Fe)	تفاوت فراوانی‌ها (Fo-Fe)
بسیار ضعیف	۱۵	۴۲/۹	۷	۸
ضعیف	۹	۲۵/۷	۷	۲
متوسط	۴	۱۱/۴	۷	-۳
خوب	۶	۱۷/۱	۷	-۱
بسیار خوب	۱	۳	۷	-۶

جدول شمارهٔ ۱ نشان می‌دهد که از بین گروه نمونه، ۴۳ درصد گزینهٔ بسیار ضعیف، ۲۶ درصد ضعیف، ۱۱ در صد متوسط، ۱۷ درصد خوب، و ۳ درصد بسیار خوب را انتخاب کرده‌اند. برای استنباط آماری در مورد داده‌های جدول ۱، از آزمون مجذور خی (کای) استفاده شده است:

$P=۰/۰۰۳$ $df=۴$ $X^2_{ob} = ۱۶/۲۸۶$ $X^2_{cr} = ۹/۴۸۸$

اطلاعات به‌دست آمده نشان می‌دهد که مجذور خی مشاهده شده (۲۸۶/۱۶) بزرگ‌تر از مجذور خی بحرانی (۹/۴۸۸) و سطح معنی‌داری (سطح احتمال) ناشی از آن (۰/۰۰۳) کوچک‌تر از سطح معنی‌داری محقق ($\alpha = ۰/۰۵$) است. پس فرض صفر رد و فرض مقابل پذیرفته می‌شود. بنابراین می‌توان نتیجه گرفت که با ۹۵ درصد اطمینان عملکرد مؤسسه‌های پژوهشی دولتی شهر تهران از نظر شاخص‌های ایزو در زمینهٔ مدیریت امنیت اطلاعات ضعیف است.

در ادامه، به منظور درک نقاط ضعف و قوت عملکرد مؤسسه‌های پژوهشی دولتی شهر تهران، نتایج آزمون هریک از شاخص‌ها به تفکیک ارائه می‌شود:

شاخص اول: سیاست امنیت اطلاعات

این شاخص یک مؤلفه دارد که درصد فراوانی نسبی آن در جدول شمارهٔ ۲ آمده است:

جدول ۲. درصد فراوانی نسبی مؤلفه‌های شاخص اول

شاخص	مؤلفه	درصد فراوانی نسبی عملکرد مؤسسه‌ها				
		بسیار خوب	خوب	متوسط	ضعیف	بسیار ضعیف
۱. سیاست امنیت	سیاست امنیت اطلاعات	۲/۹	۱۱/۴	۵/۷	۸/۶	۷۱/۴

مجذور خی مشاهده شدهٔ آزمون(۵۸/۵۷۱) بزرگ‌تر از مجذور خی بحرانی (۹/۴۸۸)، و سطح معنی‌داری ناشی از آن (۰/۰۰۰) کوچک‌تر از سطح معنی‌داری محقق (α=۰/۰۵) است. بنابراین می‌توان نتیجه گرفت که با ۹۵ درصد اطمینان عملکرد مؤسسه‌های پژوهشی دولتی شهر تهران از نظر شاخص‌های ایزو در زمینهٔ سیاست امنیت اطلاعات ضعیف است.

از آنجا که نخستین گام در مدیریت مؤثر در هر مؤسسه‌ای تعیین خط‌مشی است، عدم توجه مؤسسه‌های پژوهشی به تدوین سیاست امنیت اطلاعات بیانگر زیربنای بسیار ضعیف مدیریت امنیت اطلاعات در این مؤسسه‌ها را نشان می‌دهد. علی‌رغم گسترش نظام‌های پیشرفتهٔ اطلاعاتی و قوانین آن، تصور گستردگی و پیچیدگی نظام‌های اطلاعاتی نمی‌بایست از تهیهٔ سیاست رسمی و دارای ضمانت اجرایی در سراسر سازمان، ولو به صورت مقدماتی، جلوگیری نماید؛ و لازم است هر مؤسسهٔ پژوهشی برای پیشبرد اهداف خود و اجرای مدیریت استراتژیک اطلاعات در اولین گام اهداف کوتاه مدت و بلند مدت را تعریف و بر این اساس رویه‌های اجرایی برای مدیران و کارکنان طراحی نماید. همچنین قوانینی را برای سنجش عملکرد مؤسسه با معیارهای پذیرفته شدهٔ بین‌المللی، ملی، و یا داخل سازمانی وضع نماید.

از این لحاظ، با توجه به نتایج بدست آمده، عمده‌ترین نقطه ضعف عملکرد مؤسسه‌های مورد اشاره در زمینهٔ مدیریت امنیت اطلاعات بی‌توجهی نسبت به تهیه و تدوین سیاست امنیت اطلاعات در سازمان بوده است.

شاخص دوم: امنیت سازمانی

این شاخص سه مؤلفه دارد، که درصد فراوانی نسبی آنها در جدول شمارهٔ ۳ آمده است:

جدول ۳. درصد فراوانی نسبی مؤلفه‌های شاخص دوم

شاخص	مؤلفه	درصد فراوانی نسبی عملکرد مؤسسه‌ها				
		بسیار خوب	خوب	متوسط	ضعیف	بسیار ضعیف
۲. امنیت سازمانی	زیرساخت امنیت اطلاعات	۰/۰	۵/۷	۱۱/۴	۳۱/۴	۵۱/۴
	امنیت دسترسی شخص ثالث	۵/۷	۴۸/۵	۱۷/۱	۲۲/۸	۲/۸
	واگذاری‌ها	۰/۰	۱۴/۲	۲۰/۲	۲۲/۸	۴۰/۰

مجذور خی مشاهده شدهٔ آزمون (۸/۲۸۶) کوچک‌تر از مجذور خی بحرانی (۹/۴۸۸)، و سطح معنی‌داری ناشی از آن (۰/۰۸۲) بزرگ‌تر از سطح معنی‌داری محقق (α = ۰/۰۵) است. بنابراین می‌توان نتیجه گرفت که هرچند درصد محسوسی معتقدند که در زمینهٔ مدیریت امنیت سازمانی بسیار ضعیف عمل شده است، اما این مقدار از نظر آزمون آماری به قدری نیست که بتوان این ادعا را تأیید کرد.

شاخص سوم: امنیت اموال سازمان

این شاخص دو مؤلفه دارد، که درصد فراوانی نسبی آنها در جدول شمارهٔ ۴ آمده است:

جدول ۴. درصد فراوانی نسبی مؤلفه‌های شاخص سوم

شاخص	مؤلفه	درصد فراوانی نسبی عملکرد مؤسسه‌ها				
		بسیار خوب	خوب	متوسط	ضعیف	بسیار ضعیف
۲. امنیت اموال	مسئولیت اموال	۸/۵	۶۵/۷	۱۷/۱	۸/۵	۰/۰
سازمان	رده‌بندی اموال اطلاعاتی	۲/۸	۸/۵	۱۱/۴	۴۲/۸	۳۴/۲

مجذور خی مشاهده شدهٔ آزمون (۱۰/۰۰۰) بزرگ‌تر از مجذور خی بحرانی

(۹/۴۸۸)، و سطح معنی‌داری ناشی از آن (۰/۰۴۰) کوچک‌تر از سطح معنی‌داری محقق (α=۰/۰۵) است. بنابراین، می‌توان نتیجه گرفت که با ۹۵ درصد اطمینان عملکرد مؤسسه‌های پژوهشی دولتی شهر تهران از نظر شاخص‌های ایزو در زمینهٔ مدیریت امنیت اموال سازمان خوب بوده است.

البته این نتیجه شاید متأثر از عملکرد خوب مؤسسه‌های پژوهشی از نظر مسئولیت اموال بوده باشد که نتیجهٔ آزمون را به سمت خوب سوق داده است، ولی از نظر مؤلفهٔ دوم (رده‌بندی اموال اطلاعاتی)، هنوز نمی‌توان عملکرد آنها را رضایت بخش دانست. بنابراین، لازم است که این مؤسسه‌ها به رده‌بندی و تعیین ارزش اموال اطلاعاتی اهمیت بیشتری دهند تا بتوانند بر حسب میزان حساسیت و ارزش اطلاعات تمهیدات امنیتی مناسب را به‌کار گیرند. به این ترتیب، با صرف حداقل سرمایه، حداکثر سوددهی حاصل شده و از اتلاف سرمایه در مدیریت امنیت اموال غیرحساس و یا کم‌ارزش جلوگیری می‌گردد.

شاخص چهارم: امنیت کارکنان

این شاخص سه مؤلفه دارد، که درصد فراوانی نسبی آنها در جدول شمارهٔ ۵ آمده است:

جدول ۵. درصد فراوانی نسبی مؤلفه‌های شاخص چهارم

شاخص	مؤلفه	درصد فراوانی نسبی عملکرد مؤسسه‌ها				
		بسیار خوب	خوب	متوسط	ضعیف	بسیار ضعیف
۴. امنیت کارکنان	امنیت در شرح وظایف	۰/۰	۸/۵	۰/۰	۶۰/۰	۳۱/۴
	آموزش کاربر	۲/۸	۲/۸	۲/۸	۲۸/۵	۶۲/۸
	مسئولیت حوادث امنیتی	۰/۰	۱۴/۲۵	۲/۸	۵۴/۲	۲۸/۵

مجذور خی مشاهده شدهٔ آزمون (۳۱/۱۴۳) بزرگ‌تر از مجذور خی بحرانی (۹/۴۸۸)، و سطح معنی‌داری ناشی از آن (۰/۰۰۰) کوچک‌تر از سطح معنی‌داری محقق (α = ۰/۰۵)

است. بنابراین، می‌توان نتیجه گرفت که با ۹۵ درصد اطمینان عملکرد مؤسسه‌های پژوهشی دولتی شهر تهران از نظر شاخص‌های ایزو در زمینهٔ مدیریت امنیت کارکنان ضعیف بوده است. لذا با اشاره به این نکته که بیش از یک سوم نقص‌های امنیتی نظام‌های رایانه‌ای، طبق مطالعات انجام شده، ناشی از کارمندان است (لونی، ۲۰۰۲، ص ۳) لازم است مدیران این نوع مؤسسه‌ها توجه بیشتری نسبت به امنیت کارمندان و نیز آموزش و آگاه‌ساختن ایشان از حوادث و تهدیدهای امنیتی و روش مقابله با آنها داشته باشند تا با همکاری کارکنان امنیت مؤثری برای سازمان حاصل آید.

شاخص پنجم: امنیت فیزیکی و محیطی

این شاخص سه مؤلفه دارد، که درصد فراوانی نسبی آنها در جدول شمارهٔ ۶ آمده است:

جدول ۶. درصد فراوانی نسبی مؤلفه‌های شاخص پنجم

شاخص	مؤلفه	درصد فراوانی نسبی عملکرد مؤسسه‌ها				
		بسیار خوب	خوب	متوسط	ضعیف	بسیار ضعیف
۵. امنیت	نواحی ایمن	۲/۸	۱۴/۲	۱۱/۴	۳۱/۴	۴۰/۰
	امنیت تجهیزات	۵/۷	۴۸/۵	۳۴/۲	۸/۵	۲/۸
	فیزیکی و محیطی	۵/۷	۴۰/۰	۴۲/۸	۵/۷	۵/۷

مجذور خی مشاهده شدهٔ آزمون (۹/۱۴۳) کوچک‌تر از مجذور خی بحرانی (۹/۴۸۸)، و سطح معنی‌داری ناشی از آن (۰/۰۵۸) بزرگ‌تر از سطح معنی‌داری محقق ($\alpha = ۰/۰۵$) است. بنابراین، می‌توان نتیجه گرفت که هرچند درصد محسوسی معتقدند که در زمینهٔ مدیریت امنیت فیزیکی و محیطی خوب عمل شده است، این مقدار از نظر آزمون آماری به قدری نیست که بتوان ادعا کرد که عملکرد مؤسسه‌های مورد پژوهش از این لحاظ خوب بوده است.

البته این نتیجه متأثر از عملکرد خوب مؤسسه‌های پژوهشی از نظر امنیت تجهیزات

و کنترل‌های عمومی است. در واقع، این مؤسسه‌ها اگرچه به شکل سنتی در تأمین امنیت فیزیکی تجهیزات و ایجاد کنترل‌های عمومی برای عبور و مرور افراد، موفق بوده‌اند ولی خصوصاً با ظهور و توسعهٔ فن‌آوری اطلاعات و لزوم اختصاص نواحی ایمن برای امنیت آنها هنوز اقدام خاصی انجام نداده‌اند. بنابراین، لازم است در طراحی و معماری امنیت اطلاعات به این امر اهمیت داده شود.

شاخص ششم: مدیریت ارتباطات و عملیات

این شاخص هفت مؤلفه دارد، که درصد فراوانی نسبی آنها در جدول شمارهٔ ۷ آمده است:

جدول شماره ۷. درصد فراوانی نسبی مؤلفه‌های شاخص ششم

شاخص	مؤلفه	درصد فراوانی نسبی عملکرد مؤسسه‌ها				
		بسیار خوب	خوب	متوسط	ضعیف	بسیار ضعیف
۶. مدیریت ارتباطات و عملیات	رویه‌ها و وظایف اجرایی	۰/۰	۸/۵	۱۱/۴	۵۱/۴	۲۸/۵
	برنامه‌ریزی و پذیرش سیستم	۲/۸	۱۱/۴	۱۷/۱	۴۰/۰	۲۸/۵
	حفاظت در برابر نرم‌افزارهای خرابکار	۵/۷	۵۱/۴	۲۸/۵	۱۱/۴	۲/۸
	اداره سیستم (پشتیبانی)	۲/۸	۴۵/۷	۳۴/۲	۸/۵	۸/۵
	مدیریت شبکه	۲۵/۸	۳۴/۲	۲۸/۵	۱۴/۲	۲۰/۱
	امنیت و مدیریت رسانه	۲/۸	۱۷/۱	۲۸/۵	۲۵/۷	۲۵/۷
	تبادل اطلاعات و نرم‌افزار	۰/۰	۲/۸	۵/۷	۶۲/۸	۲۸/۵

مجذور خی مشاهده شدهٔ آزمون (۸/۰۰۰) کوچک‌تر از مجذور خی بحرانی (۹/۴۸۸)، و سطح معنی‌داری ناشی از آن (۰/۰۹۲) بزرگ‌تر از سطح معنی‌داری محقق ($\alpha = ۰۵/۰$) است. بنابراین، می‌توان نتیجه گرفت که هرچند درصد محسوسی معتقدند که در زمینهٔ مدیریت امنیت ارتباطات و عملیات ضعیف عمل شده است، این مقدار از نظر آزمون آماری به قدری نیست که بتوان این ادعا را تأیید کرد.

در واقع، اگرچه عملکرد مؤسسه‌های مذکور از نظر مؤلفه‌های سوم تا ششم به زعم مدیران موفقیت‌آمیز بوده است، ولی شاید دلیل این نوع اظهارنظرها را بتوان ناشی از ماهیت خود مؤلفه‌ها دانست. به‌طور مثال، فرض تجهیز رایانه‌ها به نرم‌افزار کشف ویروس، به خودی خود به مفهوم استفادهٔ مؤثر از آنها نیست، بلکه مستلزم آن است که این نرم‌افزارها با توجه به زمان و محل استفاده خود در پیشگیری از حوادث امنیتی مفید واقع شوند. از سوی دیگر، می‌توان اشاره کرد که با توجه به استفاده از نظام‌های نوین مدیریت و فن‌آوری اطلاعات در مؤسسه‌های مذکور، در حال حاضر بستر مناسبی برای حرکت به سوی اجرای مدیریت امنیت ارتباطات و عملیات فراهم شده است.

شاخص هفتم: مدیریت کنترل دسترسی

این شاخص هشت مؤلفه دارد، که درصد فراوانی نسبی آنها در جدول شمارهٔ ۸ آمده است:

جدول ۸. درصد فراوانی نسبی مؤلفه‌های شاخص هفتم

شاخص	مؤلفه	درصد فراوانی نسبی عملکرد مؤسسه‌ها				
		بسیار خوب	خوب	متوسط	ضعیف	بسیار ضعیف
۷. کنترل دسترسی	مقررات اداری کنترل دسترسی	۲/۸	۴۰/۰	۲۲/۸	۱۷/۱	۱۷/۱
	مدیریت دسترسی کاربر	۵/۷	۲۵/۷	۱۴/۲	۲۵/۷	۲۸/۵
	وظایف کاربر (جلب همکاری)	۰/۰	۵/۷	۲/۸	۳۴/۲	۵۷/۱
	کنترل دسترسی به شبکه	۵/۷	۵۱/۴	۱۷/۱	۱۴/۲	۱۱/۴
	کنترل دسترسی به سیستم عامل	۲/۸	۵/۷	۳۱/۴	۴۰/۰	۲۰/۰
	کنترل دسترسی به برنامه‌های کاربردی	۲/۸	۴۰/۰	۱۷/۱	۳۱/۴	۸/۵
	نظارت بر دسترسی و استفاده از سیستم	۲/۸	۵/۷	۲/۸	۳۱/۴	۵۷/۱
	تسهیلات سیار و کار از راه دور	۰/۰	۰/۰	۰/۰	۰/۰	۱۰۰/۰

مجذور خی مشاهده شدهٔ آزمون (۱۱/۴۲۹) بزرگ‌تر از مجذور خی بحرانی (۹/۴۸۸)، و سطح معنی‌داری ناشی از آن (۰/۰۲۲) کوچک‌تر از سطح معنی‌داری محقق (α = ۰/۰۵) است. بنابراین، می‌توان نتیجه گرفت که با ۹۵ درصد اطمینان عملکرد مؤسسه‌های پژوهشی دولتی شهر تهران از نظر شاخص‌های ایزو در زمینهٔ مدیریت کنترل دسترسی با اطلاعات سازمان ضعیف بوده است.

نتایج به‌دست آمده مبیّن آن است که اگرچه اقداماتی در زمینهٔ کنترل دسترسی صورت گرفته است، اما احتمالاً این اقدامات اصولی نبوده و بر حسب نیاز مقررات و اقداماتی اعمال شده است. لازم به ذکر است که اظهارنظر دربارهٔ مؤلفهٔ آخر این شاخص باید با این ملاحظه مدنظر قرار گیرد که در بسیاری از مؤسسه‌ها اصولاً کاربرد این نوع تسهیلات معمول نشده است و پاسخ‌های به‌دست آمده لزوماً به مفهوم عدم رعایت مسائل امنیتی نیست. با گسترش ساختارهای سازمانی غیرمتمرکز به‌زعم دیلون[1] و بک هاوس[2]، لازم است این مؤلفه را نیز در معماری امنیت اطلاعات در دستور کار خویش قرار دهند (دیلون و بک‌هاوس، ۲۰۰۰، ص ۱۲۵).

شاخص هشتم: گسترش و نگهداری سیستم‌ها

این شاخص پنج مؤلفه دارد، که درصد فراوانی نسبی آنها در جدول شمارهٔ ۹ آمده است:

جدول ۹. درصد فراوانی نسبی مؤلفه‌های شاخص هشتم

شاخص	مؤلفه	درصد فراوانی نسبی عملکرد مؤسسه‌ها				
		بسیار خوب	خوب	متوسط	ضعیف	بسیار ضعیف
۸. گسترش و نگهداری سیستم‌ها	الزامات امنیتی سیستم‌ها	۰/۰	۸/۵	۱۴/۲	۳۱/۴	۴۵/۷
	امنیت در سیستم‌های کاربردی	۰/۰	۱۴/۲	۸/۵	۱۷/۱	۶۰/۰
	کنترل‌های رمزنگار	۰/۰	۰/۰	۲/۸	۲/۸	۹۱/۴
	امنیت فایل‌های سیستمی	۰/۰	۲۲/۸	۱۱/۴	۳۱/۴	۳۴/۲
	امنیت در فرایندهای توسعه و پشتیبانی	۲/۸	۲۲/۸	۱۴/۲	۴۰/۰	۲۰/۱

1. Dhillon
2. Backhouse

مجذور خی مشاهده شدهٔ آزمون (۲۵/۱۴۳) بزرگ‌تر از مجذور خی بحرانی (۹/۴۸۸)، و سطح معنی‌داری ناشی از آن (۰/۰۰۰) کوچک‌تر از سطح معنی‌داری محقق (α = ۰/۰۵) است. بنابراین، می‌توان نتیجه گرفت که با ۹۵ درصد اطمینان عملکرد مؤسسه‌های پژوهشی دولتی شهر تهران از نظر شاخص‌های ایزو در زمینهٔ مدیریت امنیت گسترش و نگهداری سیستم‌ها ضعیف بوده است.

شاید یکی از دلایل این امر را بتوان عدم نیاز به توسعهٔ سیستم‌ها در شرایط فعلی دانست. در واقع، در حال حاضر در نخستین مراحل شکل‌گیری مدیریت اطلاعات در مؤسسه‌های مذکور هستیم و مسائل امنیتی مربوط به گسترش سیستم‌ها هنوز مبهم است. به هر حال علی‌رغم حصول این نتیجه می‌توان امیدوار بود که با اعمال اصلاحات امنیتی در مرحلهٔ طراحی برای گسترش و نگهداری سیستم‌ها بتوان از وقوع شکست‌های امنیتی در گام‌های بعدی جلوگیری کرد.

شاخص نهم: مدیریت تداوم عملیاتی

این شاخص یک مؤلفه دارد، که درصد فراوانی نسبی آنها در جدول شمارهٔ ۱۰ آمده است:

جدول ۱۰. درصد فراوانی نسبی مؤلفه‌های شاخص نهم

شاخص	مؤلفه	درصد فراوانی نسبی عملکرد مؤسسه‌ها				
		بسیار خوب	خوب	متوسط	ضعیف	بسیار ضعیف
۹. مدیریت تداوم عملیاتی	جنبه‌های مدیریت تداوم عملیاتی	۲/۸	۲/۸	۲/۸	۱۱/۴	۸۰/۰

مجذور خی مشاهده شده آزمون (۷۹/۷۱۴) بزرگ‌تر از مجذور خی بحرانی (۹/۴۸۸)، و سطح معنی داری ناشی از آن (۰/۰۰۰) کوچک‌تر از سطح معنی‌داری محقق (α = ۰/۰۵) است. بنابراین، می‌توان نتیجه گرفت که با ۹۵ درصد اطمینان عملکرد مؤسسه‌های مورد پژوهش از نظر شاخص‌های ایزو در زمینهٔ مدیریت تداوم

عملیاتی ضعیف بوده است.

نظر به اهمیت مدیریت تداوم عملیاتی و طراحی تمهیدات لازم برای پیشگیری از وقفه‌های کاری و تجاری، لازم است مؤسسه‌ها توجه بیشتری به این امر معطوف دارند. خصوصاً در شرایط رقابتی دنیای فعلی تجارت الکترونیکی، مدیریت بحران همراه با ارزیابی خطرات یکی از اولویت‌های سازمان‌ها در برنامه‌ریزی و اجرای مدیریت امنیت اطلاعات به‌شمار می‌رود.

شاخص دهم: مدیریت قوانین امنیتی

این شاخص سه مؤلفه دارد، که درصد فراوانی نسبی آنها در جدول شمارهٔ ۱۱ آمده است:

جدول ۱۱. درصد فراوانی نسبی مؤلفه‌های شاخص دهم

شاخص	مؤلفه	درصد فراوانی نسبی عملکرد مؤسسه‌ها				
		بسیار خوب	خوب	متوسط	ضعیف	بسیار ضعیف
۱۰. مدیریت قوانین امنیتی	هماهنگی با قوانین امنیتی	۰/۰	۸/۵	۸/۵	۳۷/۱	۴۵/۷
	نظارت بر سیاست امنیت و قوانین فنی	۰/۰	۱۴/۲	۱۴/۲	۳۴/۲	۳۴/۲
	ملاحظات حسابرسی سیستم	۲/۸	۰/۰	۰/۰	۱۷/۱	۷۷/۱

مجذور خی مشاهده شده آزمون (۳۰/۵۷۱) بزرگ‌تر از مجذور خی بحرانی (۹/۴۸۸)، و سطح معنی‌داری ناشی از آن (۰/۰۰۰) کوچک‌تر از سطح معنی‌داری محقق (α = ۰/۰۵) است. بنابراین، می‌توان نتیجه گرفت که با ۹۵ درصد اطمینان عملکرد مؤسسه‌های پژوهشی دولتی شهر تهران از نظر شاخص‌های ایزو در زمینهٔ مدیریت قوانین امنیتی و فنی ضعیف بوده است.

با توجه به گسترش قوانین بسیار متعدد بین‌المللی، امروزه پیروی از قوانین و استانداردها و نیز وضع قوانین ملی بی‌شک یکی از مهم‌ترین وظایف دولت‌هاست.

علی‌رغم عملکرد ضعیف مؤسسه‌های پژوهشی طبق نتایج به‌دست آمده، شاید بتوان دلیل آن را عدم‌توجه دولت در وضع قوانین مناسب ملی و عدم‌حضور فعال در عرصه‌های بین‌المللی و نیز بی‌توجهی نسبت به گسترش و تبادل اطلاعات و پذیرش ضوابط بین‌المللی دانست. لذا شاید بهتر باشد ابتدا دولت نسبت به توسعهٔ نظام اطلاع‌رسانی کشور و به رسمیت شناساندن آن در نظام‌های اطلاعاتی جهانی سرمایه‌گذاری نماید، سپس عملکرد مؤسسه‌های پژوهشی و سایر نهادهای دولتی و خصوصی بر طبق قوانین موضوعه مجدداً مورد ارزیابی قرار گیرد. در مجموع، عدم اطلاع مؤسسه‌های مذکور حتی از وجود چنین ضوابط و استانداردهایی به‌منزلهٔ نقطهٔ ضعف در عملکرد آنها محسوب می‌گردد.

حال با مقایسه‌ای اجمالی می‌توان نتیجه گرفت که اگرچه مؤسسه‌های مذکور در کنترل حوادث امنیتی موفق بوده‌اند؛ اما نتایج تحلیلی آزمون همچنان بیانگر آن است که اقدام جدی نیز در این زمینه صورت نگرفته است. شاید دلیل این امر این باشد که مؤسسه‌های مورد اشاره اصولاً تجربه‌ای از حوادث پرهزینه امنیتی نداشته اند؛ یا اعمال کنترل‌های امنیتی در حد افراط و مغایر با اهداف اطلاعاتی بوده؛ و یا اینکه با ورود امکانات الکترونیکی نوین هنوز انگیزه و فرصتی برای نفوذ به سیستم اطلاعات مؤسسه، برای نفوذگران به‌دست نیامده است.

نتیجه‌گیری

یافته‌ها بیانگر آن است که با ۹۵ درصد اطمینان می‌توان گفت که عملکرد مؤسسه‌های پژوهشی دولتی شهر تهران از نظر رعایت استاندارد "ایزو ۱۷۷۹۹" در زمینهٔ مدیریت امنیت اطلاعات بسیار ضعیف بوده است. به عبارت دیگر، در طراحی و اجرای نظام مدیریت اطلاعات در مؤسسه‌های پژوهشی دولتی شهر تهران، شاخص‌های استاندارد ایزو در زمینهٔ مدیریت امنیت اطلاعات بسیار اندک مدّنظر قرار گرفته است.

از آنجا که استاندارد مورد اشاره مشتمل بر ده شاخص است که در هریک از مؤسسه‌های پژوهشی دولتی شهر تهران مورد ارزیابی قرار گرفته است، نتایج ذیل نیز به‌طور ضمنی به‌دست آمده است:

۱. با ۹۵ درصد اطمینان عملکرد مؤسسه‌های پژوهشی دولتی شهر تهران در تهیه و تدوین سیاست امنیت اطلاعات بسیار ضعیف بوده است.

۲. اگرچه درصد محسوسی از مدیران معتقدند که در اجرای نظام مدیریت اطلاعات به زیرساخت‌های امنیتی بسیار کم‌توجه شده است، ولی از نظر آماری نمی‌توان این ادعا را تأیید کرد.
۳. با ۹۵ درصد اطمینان عملکرد مؤسسه‌های پژوهشی دولتی شهر تهران در زمینهٔ مدیریت امنیت اموال سازمانی خوب بوده است.
۴. با ۹۵ درصد اطمینان عملکرد مؤسسه‌های مورد پژوهش در زمینهٔ مدیریت امنیت کارکنان کمتر از حد متوسط بوده است.
۵. اگرچه درصد محسوسی از مدیران معتقدند که به امنیت فیزیکی و تجهیزات توجه زیادی شده است، ولی داده‌های آماری این ادعا را تأیید نمی‌کند.
۶. اگرچه درصد محسوسی از مدیران معتقدند که به عوامل مهم در مدیریت اجرایی اطلاعات کمتر توجه شده است، ولی از نظر آماری این ادعا مورد تأیید قرار نگرفت.
۷. با ۹۵ درصد اطمینان می‌توان نتیجه گرفت که عملکرد مؤسسه‌های پژوهشی دولتی شهر تهران در زمینهٔ مدیریت کنترل دسترسی به اطلاعات سازمان ضعیف بوده است.
۸. با ۹۵ درصد اطمینان می‌توان نتیجه گرفت که عملکرد مؤسسه‌های پژوهشی دولتی شهر تهران در زمینهٔ مدیریت امنیت توسعه و نگهداری سیستم‌ها ضعیف بوده است.
۹. با ۹۵ درصد اطمینان می‌توان نتیجه گرفت که عملکرد مؤسسه‌های پژوهشی دولتی شهر تهران در زمینهٔ مدیریت تداوم عملیاتی ضعیف بوده است.
۱۰. با ۹۵ درصد اطمینان می‌توان نتیجه گرفت که عملکرد مؤسسه‌های پژوهشی دولتی شهر تهران در زمینهٔ مدیریت قوانین امنیتی و فنی ضعیف بوده است.

پیشنهادها

● برای برنامه‌ریزان و متولیان در سطح ملی، توجه به موارد ذیل پیشنهاد می‌شود:
۱. سیاست‌گذاری و برنامه‌ریزی برای استقرار نظام مدیریت امنیت اطلاعات به عنوان زیر مجموعهٔ نظام اطلاع‌رسانی کشور؛
۲. وضع قوانین امنیتی و فنی طبق استانداردهای بین‌المللی و ملی؛
۳. نظارت بر اجرای قوانین امنیتی.
● برای مدیران عالی مؤسسه‌های پژوهشی و سایر مؤسسه‌های کوچک اداری توجه به موارد ذیل پیشنهاد می‌گردد:

۱. تعریف سیاست امنیت اطلاعات؛
۲. مدیریت امنیت سازمان؛
۳. مدیریت امنیت اموال سازمان؛
۴. مدیریت امنیت کارکنان سازمان؛
۵. مدیریت امنیت فیزیکی و محیطی سازمان؛
۶. مدیریت امنیت ارتباطات و عملیات سازمان؛
۷. مدیریت کنترل دسترسی به اطلاعات سازمان؛
۸. مدیریت امنیت گسترش و نگهداری سیستم‌ها؛
۹. مدیریت تداوم عملیاتی؛
۱۰. مدیریت قوانین امنیتی و فنی.

● برای مدیران اجرایی مؤسسه‌های پژوهشی و سایر مؤسسه‌های کوچک اداری توجه به موارد ذیل پیشنهاد می‌شود:

۱. ارزیابی وضعیت موجود امنیت اطلاعات مؤسسه؛
۲. درک لزوم توجه و تعهد نسبت به سیاست امنیت اطلاعات؛
۳. تنظیم و پیکره بندی ایمن رایانه‌های موجود در شبکه؛
۴. نصب یک دیوارآتش در تمام سیستم‌های متصل به اینترنت؛
۵. نصب نرم افزارهای ضد ویروس در تمام رایانه‌ها؛
۶. کاهش تعداد سیستم‌هایی که امنیت آنها باید تامین شود؛
۷. تهیهٔ نسخه پشتیبان از فعالیت‌های مؤسسه؛
۸. تعیین مسئول مشخص برای اموال سازمان؛
۹. آموزش پرسنل و توجیه ایشان از نظر ضرورت توجه به تمهیدات امنیتی؛
۱۰. تأمین امنیت فیزیکی و محیطی مؤسسه و نظارت بر عبور و مرورها؛
۱۱. تعیین سطوح مجاز دسترسی برای کاربران و اشخاص ثالث؛
۱۲. تشکیل کمیتهٔ ارزیابی و مدیریت بحران.

پیشنهادهایی برای پژوهش‌های آینده

۱. کشف و شناسایی منشاء حوادث امنیتی در سازمان‌ها؛
۲. کشف انگیزه‌های نفوذ به سیستم‌های اطلاعاتی در ایران؛

۳. برآورد خسارت‌های مالی ناشی از وقوع و حوادث امنیتی اطلاعات در سطح ملی.

مآخذ

آریا، ناصر (۱۳۸۰). *حسابرسی کامپیوتری: حسابرسی شبکه‌های کامپیوتری*. تهران: سازمان حسابرسی، مرکز تحقیقات تخصصی حسابداری و حسابرسی.

بولوردی، حسن (۱۳۸۰). "تحلیل امضای دیجیتال کور گروهی". پایان‌نامه کارشناسی ارشد مهندسی برق، دانشگاه صنعتی شریف.

پور اسدی اور تاکندی، منیژه (۱۳۸۰). "بررسی نقش سیستم‌های چند عامله به منظور مدیریت امنیت". پایان‌نامه کارشناسی ارشد مهندسی برق و الکترونیک، دانشکده فنی، دانشگاه تهران.

جاودانی، تقی (۱۳۸۰). "امنیت در سرورهای وب". پایان‌نامه کارشناسی ارشد مهندسی کامپیوتر، دانشکده فنی و مهندسی، دانشگاه اصفهان.

داود آبادی، مهدی (۱۳۷۳). "طراحی سیستم رمزنگاری RSA". پایان‌نامه کارشناسی ارشد مهندسی برق و الکترونیک، دانشکده مهندسی برق، دانشگاه صنعتی شریف،

رجایی، مسعود (۱۳۷۵). "بررسی و تحلیل سیستم‌های رمزکننده آنالوگ صوت". پایان‌نامه کارشناسی ارشد مهندسی برق و مخابرات، دانشکده برق و کامپیوتر، دانشگاه صنعتی اصفهان.

رضوانی، محسن (۱۳۸۰). "توصیف سطح بالای سیاست‌های امنیتی در حفاظ". پایان‌نامه کارشناسی ارشد مهندسی کامپیوتر، دانشکده مهندسی کامپیوتر، دانشگاه صنعتی شریف.

روحانی، محمدحسین (۱۳۷۲). "طرح ایجاد شبکه‌های اطلاع‌رسانی در مراکز نظامی‌کشور". پایان‌نامه کارشناسی ارشد کتابداری و اطلاع‌رسانی، دانشکده روان‌شناسی و علوم تربیتی، دانشگاه تهران.

سلامت، حسین (۱۳۷۹). "امنیت در شبکه‌های کامپیوتری". پایان‌نامه کارشناسی ارشد مهندسی کامپیوتر، پژوهشکده فنی و مهندسی، دانشگاه امام حسین.

شهیدی، محمدمهدی (۱۳۸۱). "خلأ مدیریتی چاه ویل تکفای جهانگرد است". وب، ۳۰ (آذر): ۳-۶ و ۳۸.

شیرازی، رضا (۱۳۷۴). "اصول امنیت داده‌ها و سیستم‌ها". *خبرنامه انفورماتیک*، ۶۰ (آبان): ۱۱۰-۱۱۵.

عبدالهی ازگمی، محمد (۱۳۷۵). "طراحی و پیاده‌سازی سرویس‌های امن برای شبکه‌های کامپیوتری". پایان‌نامه کارشناسی ارشد مهندسی کامپیوتر، دانشکده مهندسی کامپیوتر، دانشگاه صنعتی شریف.

فن سلمز، اس. اچ. (۱۳۷۷). "امنیت اطلاعات در بزرگراه‌های الکترونیکی". ترجمه علی اکبر پوراحمد. *اطلاع‌رسانی*. دورهٔ سوم و چهارم، ۱۳ (بهار و تابستان): ۴۲-۵۱.

محضب، محمود (۱۳۷۳). "ایمنی ارتباطات در شبکه‌های کامپیوتری". پایان‌نامه کارشناسی ارشد

مهندسی برق و مخابرات، دانشکده فنی و مهندسی، دانشگاه تربیت مدرس.

مهرابی، مسعود؛ منوچهری قشقایی (۱۳۷۹). *مؤسسات پژوهشی کشور (بخش دولت)*. تهران: وزارت علوم تحقیقات و فناوری، مرکز تحقیقات علمی کشور.

نجفی، صیاد (۱۳۷۳). "رمزنگاری و مکانیزم‌های ایمنی در شبکه‌های کامپیوتری". پایان‌نامه کارشناسی ارشد مهندسی برق و مخابرات، دانشکده فنی و مهندسی، دانشگاه تربیت مدرس.

Barnard, Lynette; Von-Solms, Rossouw (1998). "The evaluation and certification of information security against BS7799". [abstract]. *Information Management and Computer Security*. Vol. 6, No. 2-3, P. 72-77. *LISANet*. [on line] Available: http://www.Lisanet.co.uk .[16 June 2002].

Department of Trade & Industry (2002). "Information security breaches survey 2002(ISBS)". [online] Avaiable: http://www. pwcglobal.com/ Extweb/ncsuvers. nsf/ docid [7 dec. 2002].

Dhillon, Gurpreet; Backhouse, James (2000). "Information system security management in the new millennium". *Communication of the ACM*. Vol. 43, No. 7, P:125-128.[on line] Available: http://www.acm.org. [16 June 2002].

Ho, Simon; Murray, Rob (2002). "Safeguarding information assets at financial institutions: ISO 17799, out sourced managed security services, and syber insurance. [on line] Available: http://www.Camtos.com/pdf/safeguarding-Information-Assets-Article[9Dec.2002].

Lonney, Matt(2002). "Your worst security threat: Employees'?". *ZDNet(uk)*, [on line] Available: http://www.zdnet.com.com/2100-1105-889542.html .

Von-Solms, Rossouw(1998). "Why information security is so important". [abstract]. *Information Management and Computer Security*. Vol. 6, No. 4, pp.174-177. *LISANet*. [online] Available: http://www.Lisanet.co.uk .[16 June 2002].

Rizzo, Frank. "KPMG global security survey 2002: A South African perspective". *KPMG*. [on line] Available: http://csweb.rau.ac.za/ifip/issa2002/speakers/frank_rizzo.htm .[7 dec. 2002].

Stacey, Timothy (2000). "Toward standadization of information security: BS7799". *SANS Institute*. [on line] Available: http://www.rr.sans.org/policy/standardization.php .[7 dec. 2002].