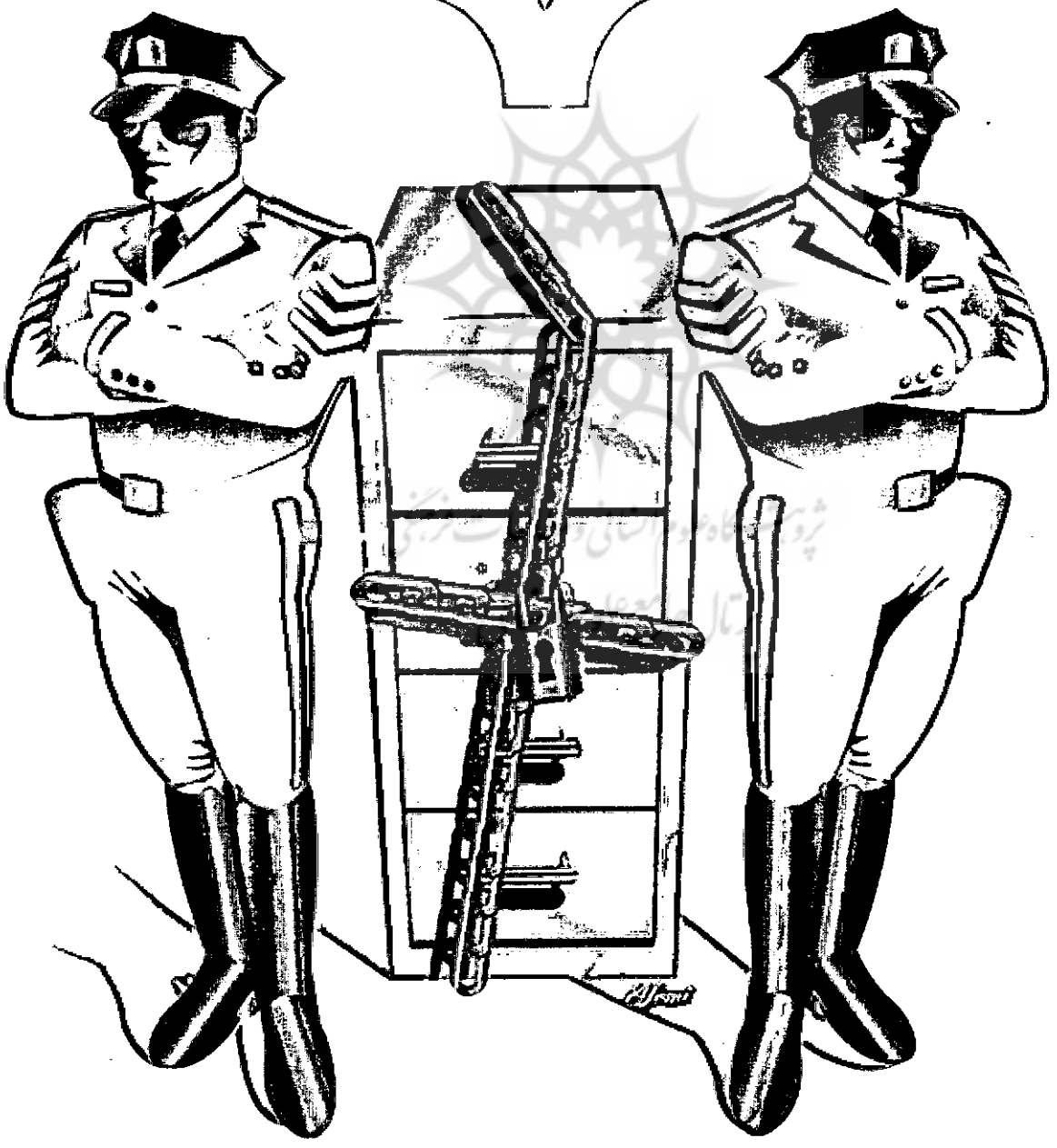
نقش مدیر عامل و هیأت مدیره در امنیت اطلاعات

پائول ویلیامز
ترجمه و تلخیص:
اسماعیل درگاهی-یوسف پاشانژاد



چکیده:
اطلاعات شرکت در هر نوع و شکل آن، جزء دارایی‌های شرکت محسوب می‌شود. این بدین معنی است که مسئولیت نهایی امنیت اطلاعات[1] باید بر عهده شرکت باشد و تنها به نقش کارمند ارشد امنیت اطلاعات[2] یا نقش‌های مشابه کفایت نشود. گرچه مسئولیت تعیین و به‌کارگیری اکثر تکنیک‌های مرتبط با امنیت اطلاعات بر عهده کارمند ارشد امنیت اطلاعات است با این حال مدیریت شرکت باید نظارت جامع[3] و مانعی برای اطمینان از اثر بخشی امنیت انجام دهد. بدون تردید مدیر عامل و هیات مدیره نقش مهمی در کشف و حذف کارشکنی‌ها دارد از طرفی باتوجه به نقش غیر قابل انکار فنآوری اطلاعات[4] دردنیای امروز، بی توجهی و سهل انگاری دراین رابطه نمی‌تواند گزینه‌ی راهبردی مناسبی باشد لذا مدیریت به ناچار باید نظارت دقیقی در این بخش داشته باشد.

کلمات کلیدی: امنیت اطلاعات، کارمند ارشد امنیت اطلاعات، فنآوری اطلاعات، مدیریت ریسک

مقدمه

در این مقاله نقش‌ها و مسئولیت‌های متنوعی که در اثربخشی امنیت اطلاعات تأثیر دارند مورد بررسی قرار می‌گیرد. انواع و اشکال متنوعی از اطلاعات وجود دارند که باید مورد حفاظت قرار گیرند، این حفاظت از گستره‌ای وسیع برخوردار است که از کوچک‌ترین واحد اطلاعات (شامل بیت و بایت دیجیتالی) شروع و تا مکالمات زبانی و رودررو را شامل می‌شود. چنانچه اطلاعات مذکور به هر نحوی در معرض خطر قرار گیرند به اعتبار شرکت لطمه وارد شده یا شرکت متحمل زیان مالی یا شکست قانونی خواهد شد.

حرکت به سمت یکپارچه سازی[5]

این عقیده مشترک میان اکثر متخصصان

> اطلاعات شرکت در هر نوع و شکل آن جزء دارایی‌های شرکت محسوب می‌شود. این بدین معنی است که مسئولیت نهایی امنیت اطلاعات باید بر عهده شرکت باشد و تنها به نقش کارمند ارشد امنیت اطلاعات یا نقش‌های مشابه کفایت نشود

امنیت اطلاعات وجود دارد که عملکرد سنتی امنیت مبتنی بر فنآوری اطلاعات در طولانی مدت مناسب نیست. در واقع نیاز و ضرورت فزاینده‌ای به ادغام و یکپارچه سازی عملکردهای متفاوت که هر یک عهده‌دار جنبه‌های خاصی از امنیت اطلاعات در شرکت‌ها است، وجود دارد به گونه‌ای که شرکت قادر به تشخیص، جلوگیری و واکنش نسبت

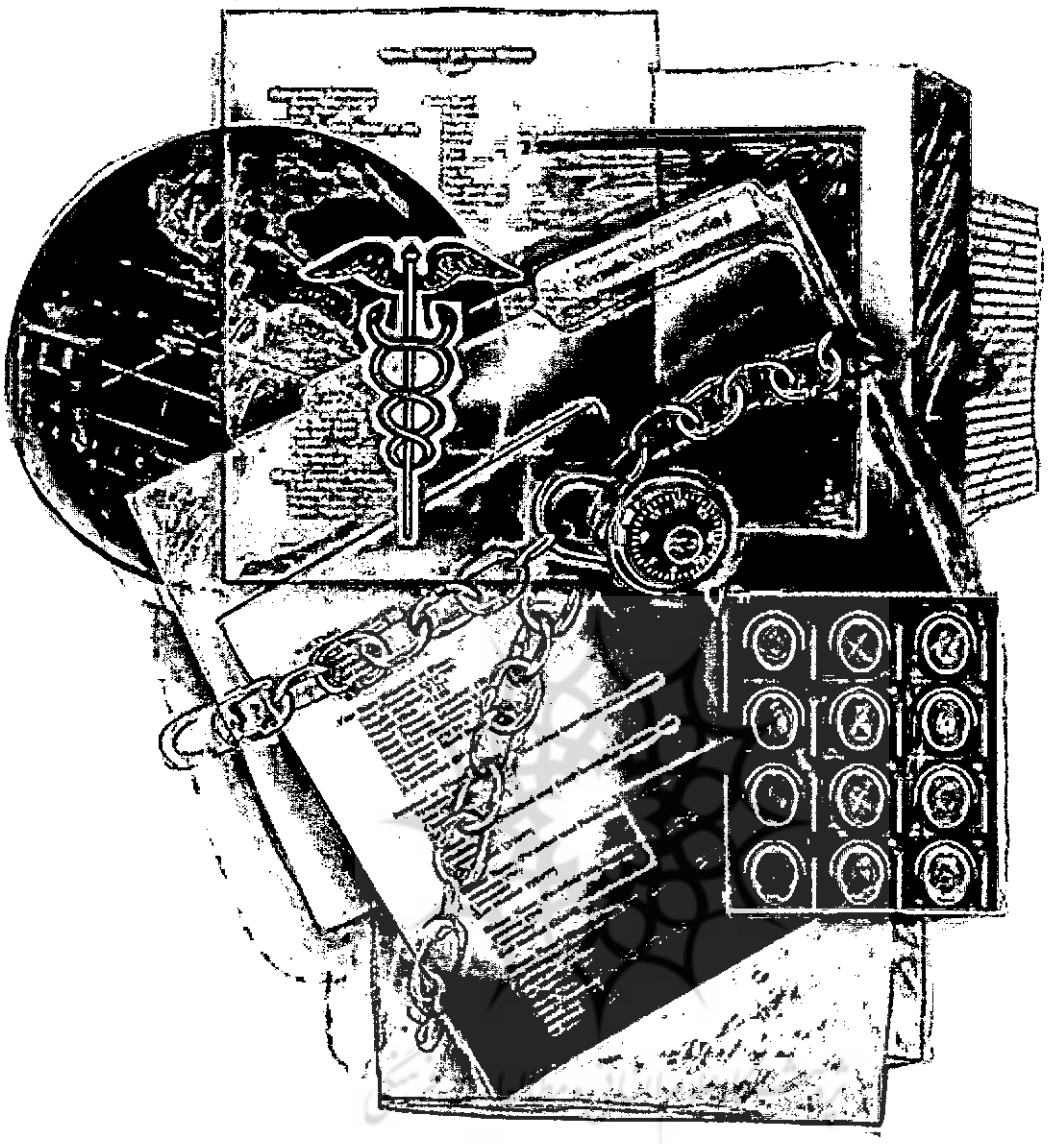
> با در نظر گرفتن زنجیره های عرضه و تامین کنندگان برون سازمانی می‌توان گفت امروزه هزاران نفر در سطوح مختلف در خارج و داخل سازمان، به نحوی در ارتباط با امنیت اطلاعات مسئولیت دارند

به هر گونه تهدید مربوط به اطلاعات شرکت یا دارایی‌های آن در هر کجا و به هر علت در سرتاسر سازمان باشد.

یکی از نمونه‌های این تفکر و گرایش ، حرکت شرکت "برتیش پترولوم"[6] در ژانویه سال ۲۰۰۷ در گردهمایی بیش از ۵۳۰ نفر از کارکنان بخش‌های امنیت اطلاعات، درخصوص امنیت شرکت و امنیت فیزیکی[7] در طی دو سال آتی به منظور ارایه طرح‌هایی برای حفاظت و حمایت از شرکت در سطح بین‌المللی است. بر اساس گزارشات منتشره، هدف شرکت مذکور از این اقدام به‌کارگیری بهترین رویکردهایی است که امنیت فیزیکی را به امنیت اطلاعات در سرتاسر شرکت مرتبط می‌سازد. این مورد تنها نمونه‌ای از مواردی است که نشان‌گر تغییر در دنیای امنیت اطلاعات در پاسخ و واکنش به فشارهای مطرح در قرن ۲۱ شامل مقررات فزاینده ، فرآیند رو به رشد جهانی شدن و تروریسم در تمام اشکال آن است. هم‌چنین استمرار روند مذکور به واسطه این پیش بینی حمایت می‌شود که در سال ۲۰۰۷ نزدیک به ۳۵٪ از ۲۰۰۰ شرکت جهانی در برای مدیریت ریسک اقدام به یکپارچه سازی امنیت اطلاعات و فعالیت‌های مداوم تجاری به منظور کنترل ریسک مالی و عملیاتی شرکت کرده‌اند.

انجمن های حرفه‌ای نیز ضرورت این موضوع را درک کرده‌اند. به عنوان مثال: می‌توان از تاسیس اتحادیه مدیریت ریسک امنیتی شرکت‌ها[8] یاد کرد که انجمن حسابرسی و کنترل سیستم‌های اطلاعاتی[9] (که گواهینامه‌های متخصصان امنیت اطلاعات را صادر می‌کند) یکی از بنیان‌گذاران آن است. اتحادیه مذکور به دنبال ارایه دیدگاه‌های جدیدی در مورد مواجه شرکت‌ها با ریسک در شرایط نیاز به یکپارچه سازی ریسک امنیت و ریسک فیزیکی است.

1 Information
2 Chief Information Security Officer
3 Overall Governance
4 Information Technology
5 Integration
6 British petroleum
7 Physical Security
8 Alliance for Enterprise Security Risk Manage
9 Information Systems Audit and Control Association



مسئولیت در سطوح سازمانی[10]

با در نظر گرفتن زنجیره های عرضه و تامین کنندگان برون سازمانی می‌توان گفت امروزه هزاران نفر در سطوح مختلف در خارج و داخل سازمان ، به نحوی در ارتباط با امنیت اطلاعات مسئولیت دارند. هر یک از این افراد دارای مسئولیت امنیتی است. به عنوان مثال: کارکنان سازمان ممکن است در جریان کارآموزی به اسناد محرمانه یا حساس شرکت به صورت غیر عمدی

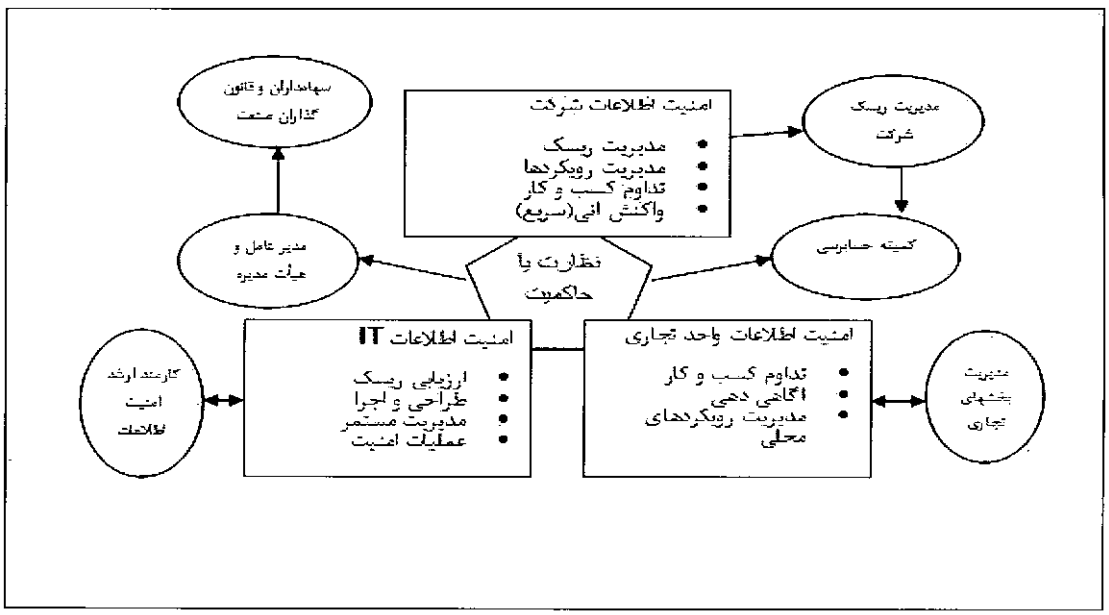
> مدیر عامل رهبری گروه مدیریت را بر عهده دارد. وی تاثیر مستقیم بر فرهنگ کنترل در کل سازمان (شرکت) داشته و سطح ریسک قابل قبول شرکت را مشخص می‌کند.

دسترسی داشته باشند و مخاطرات بعدی غیر عمدی در این مورد شکل گیرد لذا همواره باید نسبت به این مورد هوشیار بود. مدیر عامل شرکت مسئول اطمینان از این مورد است که ریسک امنیت اطلاعات شرکت به درستی درک شده و به تناسب در حال کاهش است.

در مرکز این فرایند کنترل و کاهش ریسک، متخصصان مدیریت ریسک و امنیت قرار دارند که مسئول طراحی، به‌کارگیری و مدیریت معیارهای امنیتی خاص مورد نیاز شرکت هستند. این مسئولیت از تدوین رویه‌ها تا ایجاد برنامه‌های آگاهی‌دهی امنیتی به کارکنان، گسترده است.

بنابراین افراد مسئول امنیت اطلاعات دارای نقش های متنوعی مثل رئیس هیأت مدیره ، مدیر عامل و سایر اعضای هیأت مدیره، مدیران کسب وکار، مدیران

10 Responsibilities at levels



شکل ۱: ساختار سازمانی معمول برای امنیت

ریسک، اعضای کمیته حسابرسی، اعضای کمیته امنیت، حسابرسان و کارکنان است. هر اندازه که اطلاعات برای سازمان مهم‌تر باشد به طور مستقیم نقش‌های مهم‌تری در امنیت اطلاعات وارد خواهند شد.

سرانجام کمک به ایجاد جو اطمینان از امنیت اطلاعات، وظیفه و مسئولیت هر یک از کارکنان است. به عنوان مثال به موازات آن‌که شرکت‌ها امکان دسترسی به اطلاعات را برای کارکنان در خانه، فرودگاه‌ها، محل‌های تفریح، و غیره فراهم می‌آورند، نیاز به هوشیاری و حراست مستمر در تمام سطوح بیشتر احساس می‌شود.

ضرورت امنیت

امروزه مشخص شده است که امنیت اطلاعات نقش برجسته‌ای در تجارت جهانی ایفا می‌کند. جلب اعتماد مصرف‌کننده نسبت به حفظ اطلاعات مهم و حساس وی درفرآیند روابط بلند مدت با او در تمام زمینه‌های تجاری به خصوص زمینه های خدمات مالی و بهداشتی بسیار مهم است. با این حال برخی گزارش‌ها و آمارهای منتشره همانند گزارش مرکز برنامه های اجرایی "گارتنر" در مورد کارمندان ارشد اطلاعات[11] (۲۰۰۷) حاوی مطالب متفاوتی است که در آن بیان شده، امنیت اطلاعات از ده اولویت اصلی بسیاری از

سرانجام کمک به ایجاد جو اطمینان از امنیت اطلاعات، وظیفه و مسئولیت هر یک از کارکنان است. به عنوان مثال به موازات آن‌که شرکت‌ها امکان دسترسی به اطلاعات را برای کارکنان در خانه، فرودگاه‌ها، محل‌های تفریح، و غیره فراهم می‌آورند، نیاز به هوشیاری و حراست مستمر در تمام سطوح بیشتر احساس می‌شود.

شرکت‌ها برای اولین بار در طی سال‌های گذشته حذف شده و نیز از رتبه ۲ به رتبه ۶ در ده سرمایه‌گذاری فنآوری اصلی کاهش یافته است. آیا این امر به این دلیل است که هم اکنون امنیت کاملا تحت کنترل است و سرمایه‌گذاری‌های مورد نیاز در این زمینه به قدر کفایت صورت گرفته است.

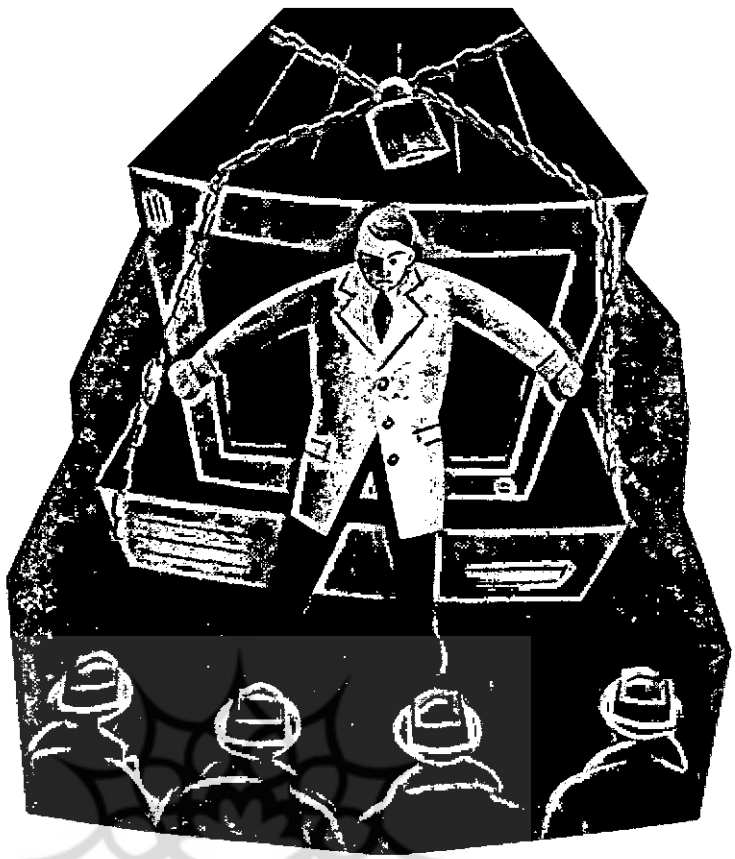
بدون تردید بسیاری از شرکت‌ها در نتیجه الزامات قانونی همانند قانون "ساربنز اوکسلی"[12]، در زمینه اطلاعات در سال‌های اخیر سرمایه‌گذاری کرده‌اند.

با این وجود آیا این واقعیت می‌تواند به مفهوم کاهش اولویت و اهمیت امنیت اطلاعات نسبت به گذشته باشد. بدون شک یک هیأت مدیره روشنفکر درک می‌کند که امنیت چیزی نیست که در نقطه زمانی خاصی در مرکز توجه قرار گیرد و سپس تا زمانی که قواعد بعدی یا بحران‌های آتی بعدی به وقوع می‌پیوندد به تعویق افتد. از دیدگاه هیأت مدیره مذکور امنیت یک فرایند مستمر است که اگرچه ممکن است میزان سرمایه‌گذاری در آن سال به سال تغییر کند با این حال میزان تمرکز و تعهد باید در هر لحظه از

11 Gartner EXP CIO۲۰۰۷ Gartner Inc (NYSE: IT) یک شرکت برتر مشاوره و تحقیقات تکنولوژی اطلاعاتی است که در زمینه موارد مربوط به تکنولوژی اطلاعات به مشتریان جهت اتخاذ تصمیمات صحیح مشاوره می دهد. گزارش سال ۲۰۰۷ این نهاد در برگیرنده نتایج حاصل از نظر سنجی ۱۴۰۰ نفر از کارکنان و مدیران ارشد اطلاعات در شرکت ها است . برای کسب اطلاعات بیشتر به آدرس مقابل مراجعه‌نمایید.

www.gartner.com

12 Sarbanes–Oxley Act



زمان در بالاترین سطح ممکن باشد. بر اساس این استدلال ضروری است که نقش‌ها و مسئولیت‌ها به‌خوبی تعریف و ساختار سازمانی به منظور اطمینان از حفظ جایگاه امنیت طراحی شود.

ساختارهای سازمانی برای امنیت

ساختار سازمانی مطلوب برای امنیت از یک شرکت به شرکت دیگر بر اساس اندازه سازمان، صنعت فعالیت، فرهنگ سازمانی و غیره متفاوت است. شکل ۱ نحوه تعیین یک ساختار سازمانی معمول در یک سازمان بین‌المللی و بزرگ را نشان می‌دهد.

گرچه ساختار سازمانی و خط‌مشی گزارش‌گری می‌تواند از یک شرکت به شرکت دیگر متفاوت باشد با این حال برخی ویژگی‌ها به صورت عمومی قابل اعمال و مشترک است. به عنوان مثال، تاکید بر امنیت اطلاعات کل شرکت مشخص می‌کند که جنبه‌های مرتبط با فنآوری اطلاعات حائز اهمیتی خاص

> مدیر ارشد اطلاعات مسئولیت مستقیم در ارتباط با امنیت اطلاعات را دارد. گرچه این وضعیت در حال تغییر است، اما هم اکنون کارمند ارشد امنیت اطلاعات به‌طور مستقیم به مدیر ارشد اطلاعات، گزارش می‌دهد.

هستند و این‌که عناصر اصلی امنیت همانند میزان توسعه یافتگی رویکردها و سیاست‌های امنیتی و واکنش‌های سریع برای بحث امنیت اطلاعات و مدیران مسئول بسیار مهم است. به طور مشابه درک این نکته مهم است که؛ خطوط تجاری متفاوت و یا خطوط تجاری مستقر در بخش های جغرافیایی گوناگون ممکن است نیازهای متفاوتی داشته باشند.

ساختار معمولی (امنیت) مستلزم وجود عملکرد متمرکز در مورد ریسک شرکت[13] است که چنین عملکردی، ویژگی غالب اکثر ساختارهای سازمان‌یافته و متکی بر اطلاعات است.

با این حال مهم‌ترین موضوع در این زمینه نیاز به حاکمیت یا نظارت است که در رابطه با موارد زیر اساسی است:

تعیین مسئولیت‌ها و امتیازات تصمیم‌گیری به صورت واضح

ایجاد یک چارچوب اطمینان نسبت به شفافیت فعالیتها از طریق معیارهای مناسب

اطمینان نسبت به تامین نیازها و الزامات قانونی

اطمینان نسبت به تامین الزامات قانونی

اطمینان نسبت به این‌که منابع به صورت صحیح و مقتضی مورد استفاده قرار می‌گیرد و این‌که ارزش موردانتظار از منابع کسب شده است.

به طور کلی می‌توان گفت که عنصر حاکمیت یا نظارت همانند عاملی است که سایر عناصر امنیت را به هم مرتبط ساخته و از تبادل میان آن‌ها اطمینان معقول ایجاد می‌کند.

در رابطه با مباحث امنیت اطلاعات انجمن نظارت و حاکمیت فنآوری اطلاعات از طریق انتشارات خود — رهکرد هیات مدیره و مدیر عامل (جلد دوم) — اطلاعات و رهکردهای جامعی برای افراد مسئول در رابطه با امنیت اطلاعات فراهم می‌کند. این نشریه برای "دانلود" در سایت www.itgi.org قرار دارد.

کمیته حسابرسی

مرکز ثقل اثر بخشی حاکمیت (هم درمورد شرکت و هم در مورد فنآوری اطلاعات) در بسیاری از شرکت‌ها، کمیته حسابرسی است. گرچه بسیاری از شرکت‌های عمومی و خصوصی از سالیان قبل دارای کمیته‌های حسابرسی بوده‌اند با این حال طبق قانون "ساربنز-

13 Centralized corporate risk function

اوکسلی" داشتن کمیته مذکور جزو الزامات شرکت است.

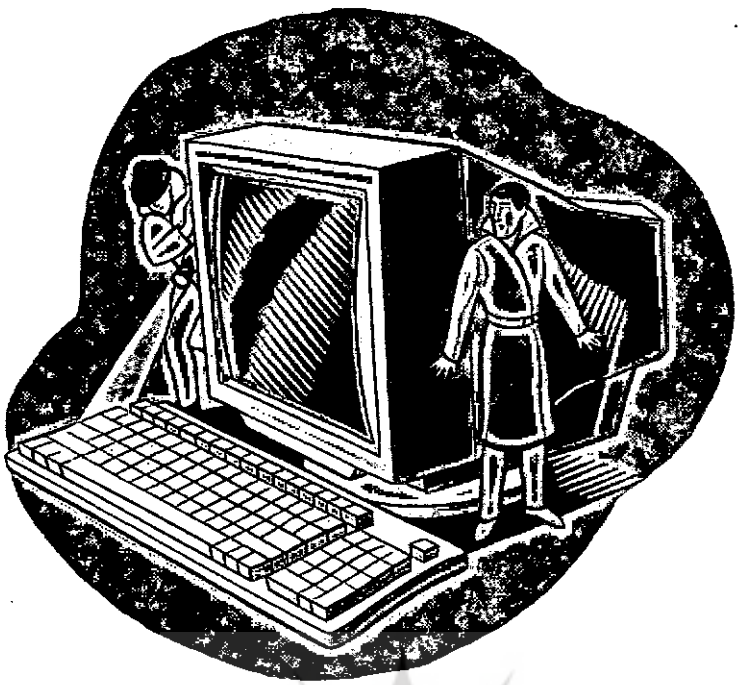
به طور سنتی کمیته حسابرسی جزو کمیته‌های فرعی هیات مدیره است. کمیته مزبور که اغلب تحت ریاست یک مدیر غیر موظف (غیر اجرایی) است، مسئول ارتباط با حسابرسان داخلی و خارجی برای کمک به حصول اطمینان از انسجام گزارش‌گری مالی است. هم‌چنین کمیته باید اطمینان حاصل کند که یک کنترل داخلی مناسب تعیین شده و به طور موثر در سازمان اجرا می‌شود.

مسئولیت فوق الذکر به واسطه قوانین و مقررات جدید تا حدی توسعه داده شده‌اند که سایر جنبه های غیر مالی را هم شامل می‌شوند. گرچه بحث امنیت اطلاعات توسط بسیاری از سازمان‌ها به عنوان جنبه اصلی کنترل داخلی در نظر گرفته شده است ولی مسئولیت‌های درنظر گرفته شده جدید برای کمیته حسابرسی، آن را در حیطه وظایف و کارکردهای کمیته حسابرسی قرار می‌دهد.

مورد اصلی در این حیطه، توان کمیته حسابرسی در درک کامل طیف وسیع مسئولیت‌ها است. بدون شک این کمیته در زمینه به چالش کشیدن و پی‌گیری موارد سوال برانگیز و دستیابی به پاسخ صحیح قابلیت‌های خاصی دارد. وجود چنین قابلیت‌هایی درنتیجه حمایت و توجه به اعضای کمیته حسابرسی و نیز اعتماد فزاینده به مشاوران برون سازمانی مثل مشاوران مدیریت ریسک مستقل و حسابرسان مستقل است. روابط ساختاری میان کارمند ارشد امنیت اطلاعات و رئیس کمیته حسابرسی و سایر متخصصان مدیریت ریسک به عنوان یک الزام اساسی برای آینده مطرح است.

نقش کارمند ارشد امنیت اطلاعات

وظیفه اصلی کارمند ارشد امنیت اطلاعات به طور معمول گزارش‌دهی



به مدیر ارشد اطلاعات یا سایر مدیران ارشد است. تمرکز فزاینده بر امنیت اطلاعات منجر به تغییر این خط‌مشی گزارش‌گری شده است. امروزه کارمند ارشد امنیت اطلاعات به ترکیبی از مدیران مانند مدیریت مالی، مدیر

> سایر مدیران کسب وکار باید مسئول امنیت اطلاعات کسب و کار البته با حمایت و پشتیبانی فعال متخصصان امنیت باشند. تنها این مدیران ماهیت مخرمانه یا حساس بودن اطلاعات را درک می‌کنند.

عملیاتی یا حتی گاهی به‌طور مستقیم به مدیر عامل شرکت گزارش می‌دهد. تغییر دیگر در این خط‌مشی گزارش‌گری، ارایه گزارش به کارمند ارشد ریسک است. در این صورت آیا نقش کارمند ارشد امنیت اطلاعات کاهش خواهد یافت؟ انتظار می رود امنیت اطلاعات مرتبط با فنآوری اطلاعات به عنوان یک الزام اصلی باقی بماند. علاوه بر این، به دلیل وابستگی اطلاعات شرکت‌ها به فنآوری دیجیتال، هم اکنون بحث امنیت اطلاعات به عنوان الزامی اساسی برای اکثر شرکت‌ها مطرح است.

به موازات تغییر فنآوری و پیچیدگی فزاینده آن و نیز افزایش تنوع اطلاعات، نیاز به مهارت‌های فنی امنیت بیشتر خواهد بود. با این وجود تأکیدی بر درک ریسک‌های تجاری گسترده‌تر و نیز محیطی که امنیت مرتبط با فنآوری اطلاعات در آن بوجود می‌آید، وجود نخواهد داشت.

به عنوان مثال کارکردها و کاربردهای امنیت در شرایط اقتصاد دیجیتال[14] و نمونه‌های تجاری جدید آن بر مبنای آزادسازی[15]، جهانی‌سازی و یکپارچه‌سازی چیست؟ نمونه‌های مذکور و سایر عوامل مرتبط ، تأثیر قابل ملاحظه‌ای بر شیوه عملکرد امنیت اطلاعاتی در آینده دارد. صرف‌نظر از تحقق یا عدم تحقق تمام ایده‌های جدید ، نقش یک کارمند ارشد امنیت اطلاعات آگاه و با اراده باید مدنظر قرار گیرد زیرا این افراد توان حمایت از هرگونه تغییر عملیاتی، مهارتی یا فرهنگی ضروری را

14 Digital economy

15 Openness

دارند. همکاری با هیأت مدیره و تفویض اختیارات از ناحیه آن‌ها بخش مهمی از نقش متخصصان امنیت را تشکیل می دهد. شرکت در دوره های آموزش مباحث نوین مدیریت ، مطالعات گسترده تجاری، آموزش و یادگیری مباحث مالی، همکاری در مناسبات تجاری راهکارهایی است که می‌تواند در افزایش کارکرد و فایده‌مندی و توان متخصصان امنیت، مفید باشد.

نقش هیأت مدیره

خصوصیت اصلی حاکمیت شرکتی تمرکز بر هیأت مدیره در حمایت از منافع تمام ذینفعان شرکت است. بنابراین از آنجا که هر یک از اعضای هیأت مدیره به صورت انفرادی تمام مهارت‌های لازم برای اطمینان از عملکرد مذکور را ندارند لذا ضروری است که به صورت مشترک و با همکاری در این حیطه عمل کنند. مهارت‌های مذکور مستلزم داشتن تخصص کافی نیست بلکه اعضای هیأت مدیره باید بدانند که چه سوالاتی را و به چه صورت از افراد مسئول در حیطه مدیریت ریسک بپرسند. هیأت مدیره باید اطمینان واضحی در مورد مدیریت ریسک در شرکت و نیز تداوم وضع مذکور کسب کند. این واقعیت به صورت اتفاقی حاصل نمی‌شود. احتمالا گزارش‌گری رسمی و قانونی از ناحیه بخش‌های مربوط شامل کمیته حسابرسی،حسابرس‌داخلی،حسابرسی خارجی و امنیت اطلاعات بخشی از این فرآیند اطمینان‌دهی را تشکیل می دهند که تماما به واسطه معیارها و فرآیندهای مناسب حمایت می‌شوند. در ادامه برخی مسولیت‌های خاص اعضای هیأت مدیره در ارتباط با امنیت اطلاعات تشریح می‌شود.

مدیر عامل

مدیر عامل رهبری گروه مدیریت را بر عهده دارد. وی تاثیر مستقیم بر فرهنگ کنترل در کل سازمان (شرکت) داشته و سطح ریسک قابل قبول شرکت را مشخص می‌کند. مدیر عامل باید میان نیاز به اختیاردهی به افراد و ایجاد شرایط بروز ابتکار و نیز نیاز به کنترل و بررسی‌ها در تمام اشکال آن که شامل امنیت نیز است، تعادل ایجاد کند. با این حال، یک مدیرعامل آگاه و روشن بین باید اهمیت امنیت در رابطه با اعتبار و شهرت شرکت را درک و اطمینان حاصل کند که منابع مناسب برای ابتکارات مرتبط با امنیت تخصیص می‌یابد.

مدیر ارشد اطلاعات

گرچه ممکن است مدیر ارشد اطلاعات به‌طور مستقیم جزو هیأت مدیره باشد با این حال باید گزارش‌دهی موثر به هیات مدیره داشته باشد. مدیر ارشد اطلاعات مسئولیت مستقیم در ارتباط با امنیت اطلاعات را دارد. گرچه این وضعیت

> کارمندان ارشد امنیت اطلاعات به تنهایی تمام مسئولیت‌های امنیت اطلاعات را بر عهده ندارند. افراد و نقش‌های متنوعی در کل سازمان از جمله رئیس هیأت مدیره، مدیر عامل و سایر اعضای هیأت مدیره، مدیران کسب وکار، متخصصان مدیریت ریسک، اعضای کمیته حسابرسی، حسابرسان و در نهایت همه کارکنان در این مسئولیت سهیم هستند.

در حال تغییر است، اما هم اکنون کارمند ارشد امنیت اطلاعات به‌طور مستقیم به مدیر ارشد اطلاعات، گزارش می‌دهد. مدیر ارشد اطلاعات هم‌چنین مسئول اطمینان در این مورد است که اعضای هیأت مدیره و سایر مدیران ارشد تجاری از عملکرد فنآوری اطلاعات به اندازه کافی برای ایفای مسئولیت های حاکمیتی فنآوری اطلاعات شامل موارد امنیت، درک و اطلاع دارند.

سایر مدیران کسب وکار[16]

سایر مدیران کسب وکار باید مسئول امنیت اطلاعات کسب و کار البته با حمایت و پشتیبانی فعال متخصصان امنیت باشند. تنها این مدیران ماهیت محرمانه یا حساس بودن اطلاعات را درک می‌کنند. در نتیجه، به منظور اجتناب از هزینه‌های اضافی و نیز ایجاد تعادل میان میزان دسترسی مقتضی و امنیت، مشارکت مستقیم مدیران تجاری در فرآیند حاکمیت امنیت حائز اهمیت است. به منظور تحقق این ایده، آموزش اصول کسب وکار برای متخصصان حرفه‌ای و نیز آموزش فنآوری اطلاعات برای مدیران ضروری است.

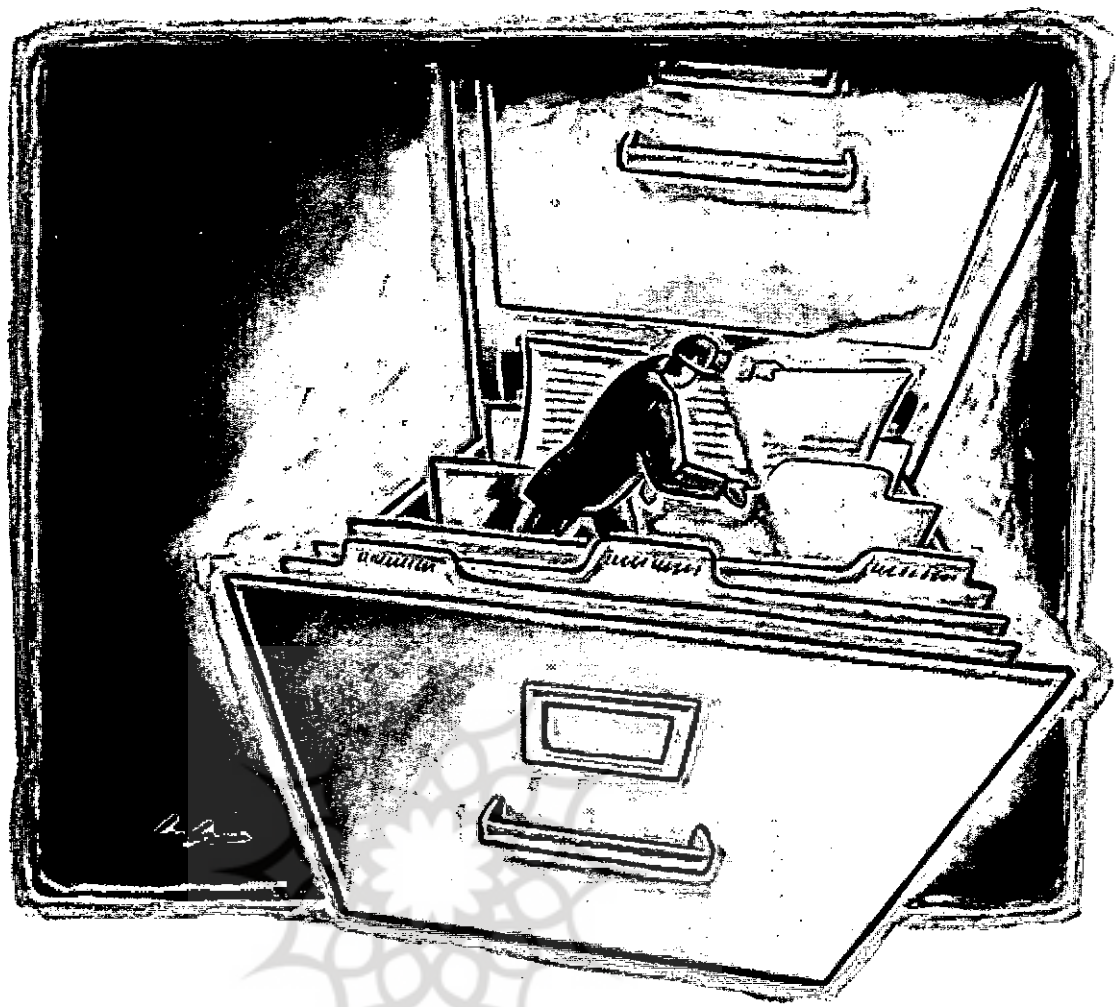
مدیران نیروی انسانی[17]

بیشتر مشکلات امنیت توسط عوامل انسانی و نه زیر ساخت‌های مهارتی صورت می‌گیرد. بنابراین لازم است مدیران نیروی انسانی[18] با نیازهای امنیتی آشنایی کافی داشته باشند. عملکرد مدیریت نیروی انسانی می‌تواند در حصول اطمینان نسبت به ایجاد و حفظ رویکردهای مناسب نیروی انسانی مفید واقع شود. به عنوان نمونه دوره‌های آموزشی کارکنان جدید باید شامل مطالبی در خصوص امنیت اطلاعات باشد.

مدیران غیر اجرایی

مدیران غیر اجرایی نیز باید نقش کلیدی در تمام جنبه های حاکمیت یا نظارت فنآوری اطلاعات شامل: امنیت ایفا کنند. انتخاب این افراد در هیأت مدیره می‌تواند به منظور پر کردن شکاف دانش میان اعضای اجرایی هیأت مدیره صورت گیرد . با این حال بررسی مدیران غیر اجرایی موسسه ارنست و یانگ[19] در سال ۲۰۰۷، مشخص کرد؛ که در ارتباط

16 Business Directors
17 Human Resource Directors
18 Human Resources
19 Ernst & Young



با امنیت اطلاعات، تعداد کمی از مدیران مذکور دارای تخصص فردی هستند. این وضعیت معمولا به حاکمیت شرکتی مربوط است و بدون تردید به عنوان ضعف ساختار هیأت مدیره جاری، تلقی می‌شود. این نقش نسبتا جدید، واکنشی برای نیاز به دیدگاه "کل نگر"[20] درمورد ریسک است. این نقش کلید اصلی در حصول اطمینان نسبت به تشخیص و مدیریت صحیح تمام ریسک‌های شرکت شامل ریسک اطلاعاتی است. فرض اصلی تمرکز مسئولیت مذکور ، توان کاهش مسئولیت‌های مدیران واحدهای تجاری انفرادی است.

نتیجه گیری

کارمندان ارشد امنیت اطلاعات به تنهایی تمام مسئولیت‌های امنیت اطلاعات را بر عهده ندارند. افراد و نقش‌های متنوعی در کل سازمان از جمله رئیس هیأت مدیره، مدیر عامل و سایر اعضای هیأت مدیره، مدیران کسب وکار، متخصصان مدیریت ریسک، اعضای کمیته حسابرسی، حسابرسان و در نهایت همه کارکنان در این مسئولیت سهیم هستند. تعدد و تنوع نقش های درگیر در امنیت اطلاعات نشان‌گر اهمیت و جایگاه حساس آن در شرکت‌ها است. بدیهی است تنوع نقش‌ها به موازات افزایش اهمیت اطلاعات برای شرکت افزایش می‌یابد. همه این افراد باید برای کنترل و کاهش ریسک‌های امنیت اطلاعات در سطح شرکت بکوشند. در مرکز این فرآیند کنترلی، متخصصان مدیریت ریسک و امنیت، نقش ویژه‌ای را از طریق طراحی، به‌کارگیری و مدیریت معیارهای امنیتی ایفا می‌کنند. از طرفی کمیته حسابرسی نیز به عنوان مرکز ثقل اثر بخشی حاکمیت شرکتی، به دلیل مسئولیت در قبال کنترل‌های داخلی و نیز موارد گزارش‌گری مالی، باید ارتباط و هماهنگی تنگاتنگی با موارد امنیت اطلاعاتی و فیزیکی در سطح سازمان داشته باشد. به عبارت دیگر روابط میان کارمند ارشد امنیت اطلاعات و رئیس کمیته حسابرسی و متخصصان مدیریت ریسک از عوامل موثر در تحقق وظیفه انسجام گزارش‌گری مالی است. در این صورت موفقیت از آن شرکت‌هایی است که نقش های مرتبط را شناسایی و پاسخ‌دهی را به صورت واضح و آشکار تعیین و ساختار حاکمیت شرکتی مناسب را فراهم کرده‌اند.