امنیت سایبری

ترجمه: دکتر حلیمه رحمانی
امیرهادی معنوی‌مقدم
The Institute of Chartered Accountants in England and Wales (ICAEW)

پیشگفتار

حسابرسی فعالیتی در جهت منافع عموم است. گزارش حسابرسان باعث به‌وجود آمدن اعتماد به صورتهای مالی می‌شود، به شرکتها اعتبار و به ذینفعان اعتماد خاطر می‌دهد. حسابرسان در طول کارشان برای حسابرسی صورتهای مالی یک شرکت، به موارد بسیاری ازجمله مسائل مربوط به داراییهای شرکت، افرادی که در شرکت کار می‌کنند و بازارهای فروش برخورد می‌کنند.

امنیت سایبری[1] کار گروهی از متخصصان حسابرسی از شرکتهای حسابرسی با اندازه بزرگ و متوسط است که سالهای زیادی تجربه در زمینه حسابرسی دارند. نمایندگانی از شرکت‌های زیر، گروه متخصصان حسابرسی این گزارش را شکل داده‌اند: **بی‌دی‌او**(BDO)، **پرایس‌واترهاوس کوپرز**(PwC)، **کی‌پی‌ام‌جی**(KPMG)، **گرنت تورنتون**(Grant Thornton)، **ارنست‌اندیانگ**(E&Y)، و **دیلویت**(Deloitte).

تغییر از **امنیت اطلاعاتی**[2] به «امنیت سایبری»، بیانگر یک تغییر عمده است. نگرشهای سنتی نسبت به مقوله امنیت اطلاعاتی، به‌منظور کسب اعتماد، درستی و دسترسی به داده‌ها بر کنترلهای داخلی تمرکز کرده‌اند. در حالی که این کنترلها همچنان وجود دارند، امنیت سایبری طیف گسترده‌تری از عوامل داخلی و خارجی را دربرمی‌گیرد:

- امروزه تهدیدهای بالقوه‌ای در سرتاسر جهان وجود دارند و می‌توانند شامل مجرمین سازمان‌یافته، نفوذگرها و جاسوسهای شرکتها و همچنین کارکنان ناراضی یا بی‌دقت باشند،
- ضعف امنیتی می‌تواند در سرتاسر یک **زنجیره تأمین**[3] و نه‌فقط در یک کسب‌وکار خاص وجود داشته باشد، و
- اثر شکستهای امنیتی می‌تواند در تمام جنبه‌های کسب‌وکار شامل اختلال در عملیات و خدمات مشتریان، اختلال در سیستمهای کنترل تولید، آسیب به نام تجاری و شهرت شرکت، دزدی داراییهای فکری یا اطلاعات تجاری حساس و جریمه‌ها گسترش یابد.

مدیریت ریسکهای سایبری برای کسب‌وکارهای فردی و همچنین گستره اقتصاد جامعه نیازمند همکاری بسیاری از ذینفعان با یکدیگر است. با به اشتراک‌گذاری دیدگاه‌ها در این گزارش، ما خواهان پشتیبانی از بحثهای عمومی شکل‌گرفته در این‌باره و کمک به مؤسسه‌های تجاری برای فهم ماهیتِ در حال تغییر تهدیدهایی هستیم که با آن دست به گریبان‌اند.

اهمیت امنیت سایبری در سالهای اخیر به‌واسطه افزایش اتکا به **فناوری اطلاعات**[4] و اینترنت، رشد چشمگیری داشته است. مباحث امنیت سایبری، مؤسسه‌های تجاری با هر اندازه‌ای و در هر حوزه‌ای را تحت تأثیر قرار می‌دهند. در این گزارش چهار حوزه‌ای که حسابرسان معتقدند بیشترین ارتباط را به مدیریت ارشد، مدیران غیراجرایی، سرمایه‌گذاران، سیاست‌گذاران و دیگر سهامداران دارد، مورد بررسی قرار می‌گیرد.

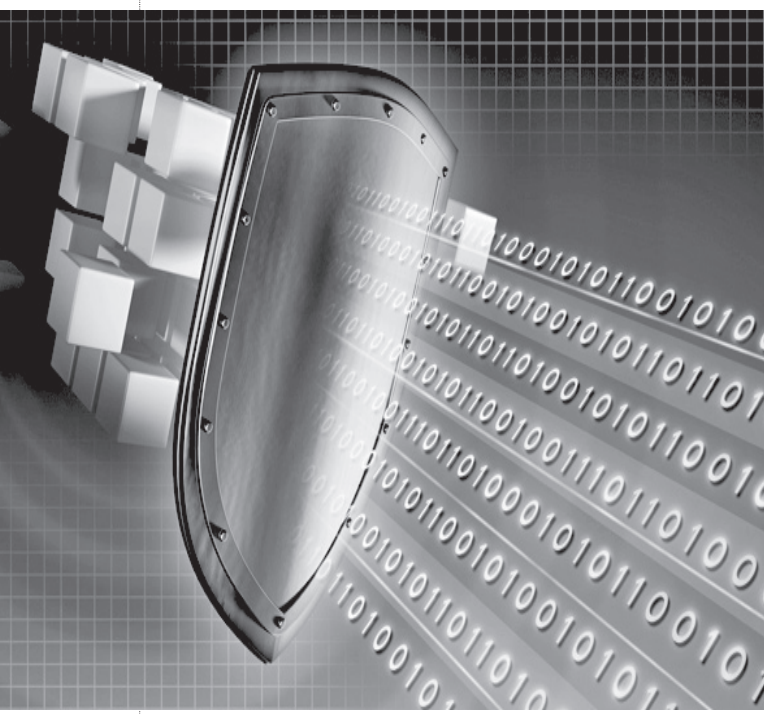
امنیت، عرصه‌ای در حال تغییر

مؤسسه‌های تجاری نیازمند افزایش تمرکز بر فعالیتهای امنیتی‌شان به‌منظور پاسخگویی به نیازهای محیط در حال تغییر کنونی هستند. به‌طور سنتی، یک مؤسسه تجاری اطراف کارخانه را دیوارکشی می‌کند و موارد امنیتی فیزیکی را در نظر می‌گیرد تا محیطی امن را به‌وجود آورد. با این حال، تغییرات در فناوری و الگوهای تجاری در سالهای اخیر، باعث شده که فضای سازمانی روزبه‌روز نفوذپذیرتر شود. تلفنهای همراه، شبکه‌های کامپیوتری به‌هم‌پیوسته، شبکه‌های اجتماعی، به‌کارگیری خدمات شبکه که از بیرون از کارخانه مدیریت می‌شود و مواردی از این‌دست، همه و همه باعث شده‌اند که مقادیر زیادی اطلاعات در خارج از شرکت و به دور از کنترل مستقیم آن، ذخیره و قابل‌دسترسی باشند. در نتیجه، بسیاری از مؤسسه‌های تجاری اطلاعات باارزش و محرمانه‌ای دارند که در اختیار عرضه‌کنندگان یا مشاوران حرفه‌ای می‌باشد و در شبکه‌های اطلاعاتی بیرون شرکت، شبکه‌های به‌هم‌پیوسته اطلاعاتی، یا کامپیوتر دستی و شخصی کارمندان قرار دارند.

این بدان معنی است که شرکتها ممکن است نیاز به وسعت بخشیدن دیدگاهشان به مقوله امنیت داشته باشند. به‌همراه حفاظت از اطلاعاتی که تحت کنترل مستقیم شرکت باقی می‌ماند، آنها ممکن است نیاز به حفاظت از اطلاعاتی داشته باشند که بیرون از مرزهای فیزیکی شرکت است و یا به‌وسیله اشخاص ثالث قابل‌دسترسی است.

دولتها علاقه‌مند به توانمندی شرکتها در محافظت از خودشان و زنجیره‌های تأمین گسترده‌شان در برابر حملات سایبری هستند. با در نظر گرفتن اهمیت اقتصاد **رقومی**[۵]، اثر شکستهای پیاپی امنیتی بر مؤسسه‌های تجاری، می‌تواند عمده باشد. در مقابل، فرصتی برای توسعه مزایای رقابتی اقتصادهای ملی به‌عنوان مکانهای مطمئن برای انجام تجارت رقومی فراهم آمده است. گذشته از این، دولتها نیاز دارند تا به‌صورت تنگاتنگی با بخش خصوصی به‌منظور ایجاد اطمینان از اینکه ریسکهای سایبری به‌درستی مدیریت شده‌اند، همکاری کنند. این بدان سبب است که بسیاری از بخشهای زیربنایی ملی مهم به‌وسیله بخش خصوصی اداره و یا مالکیت می‌شوند و مؤسسه‌های خصوصی بسیاری درون زنجیره تأمین بخشهای زیربنایی ملی حساس قرار دارند.

در نتیجه ما شاهد علاقه روزافزون دولتها به این مقوله هستیم. با توجه به سرعت تغییرات تجاری و فناوری، مقررات‌گذاری مؤثر به یک چالش بدل شده است و ریسک ذاتی و پیامدهای ناخواسته مقررات‌گذاری بیش از حد را نیز نباید از نظر دور داشت.



با این حال، اگر زیانها و شکافهای امنیتی به سیر صعودی خود ادامه دهد، احتمال دارد علاقه دولتها به این بخش نیز بیش از پیش افزایش یابد.

چهار خطمشی برای امنیت سایبری

سطح بالای ابهام درباره تهدیدهای امنیتی، تصمیم‌گیری مناسب درباره امنیت را همچنان مختل خواهد کرد و رویکردهای عمل‌گرایانه برای غلبه بر این مشکل موردنیاز خواهد بود. اطلاعات قابل‌اتکای محدودی درباره مقیاس حملات و شکافهای امنیتی و همچنین اثر واقعی آنها بر روی مشتریان، بنگاهها و کل اقتصاد وجود دارد. تحقیقها در حوزه صنایع امنیتی فناوری اطلاعات ممکن است به‌صورت اغراق‌شده و در جهت خدمت به منافع همان صنعت در نظر گرفته شوند. از طرف دیگر، سازمانهای فعال در حوزه امنیت ملی ممکن است به دلایل امنیت ملی مایل نباشند تا اطلاعاتشان را درباره حمله‌های سایبری در اختیار عموم قرار دهند و بنگاهها نیز همچنان از پذیرش چنین

حمله‌هایی اکراه دارند.

در حالی‌کـه ابتکارهایی برای تشـویق به اشـتراک‌گذاری بیشـتر اطلاعات وجود دارد، احتمال دارد فقدان شفافیت و اطلاعات خوب به‌عنوان یک چالش بزرگ باقی بماند و این خود باعث مختل شدن تصمیم‌گیریهـای تجاری و سیاسـت‌گذاریهای دولتی خواهد شـد. بنابراین به توسـعه رویکردهای متفاوت و عمل‌گرایانه برای مقابله با این سـطح بالای ابهام، نیاز خواهیم داشـت. برای مثال، تجزیه انواع مشـخصی از ریسکهای سـایبری و ایجاد پایگاه اطلاعاتی در این رابطه در مواردی که ممکن است، مفید خواهد بود.

خط‌مشـی ۱: مؤسسـه‌های تجاری باید «سایبر» را در تمام فعالیتهایشان مدنظر داشته باشند

همچنان که مؤسسـه‌های تجاری به‌صورت روزافزون به فناوری رقومی برای انجام کل عملیاتشـان وابسته می‌شوند، نیاز دارند که فرصتها و تهدیدهای مرتبط با آن را نیز درک کنند. رقومی شـدن به‌عنـوان راهی بـرای افزایش کارایی، کاهـش هزینه‌ها و تعامل بیشتر با مشتریان در نظر گرفته می‌شود. همچنین می‌تواند باعث دسـتیابی مؤسسـه‌های تجاری به بازارهای تازه و یافتن راههای نوین برای تعاملهای درون‌سـازمانی و ارتباط با شـرکای تجاری و عرضه‌کنندگان باشـد. توانایی اسـتفاده از اطلاعات مشتریان، عرضه‌کننـدگان، رقبا و دیگران به‌طـور قابل‌ملاحظه‌ای موفقیت مؤسسـه تجاری را تحت تأثیـر قرار خواهد داد. اسـتفاده از همه این شـیوه‌ها با به‌صرفه‌تر شدن بهره‌گیری از خدمات فناوری و یا ظهور نسل جدید فناوریهای نوین، سرعت خواهند گرفت.

بهره‌گیـری از فرصتهای تازه در حوزه سـایبری باعث به‌وجود آمدن چالشـهای جدیدی درباره اتکاپذیری ساختارهای رقومی و امنیت اطلاعات تجاری مهم می‌گردد. شکسـت امنیت سایبری می‌توانـد باعـث به‌وجود آمدن آسـیبهای عمده به یک مؤسسـه تجاری شـامل اختلال تجاری، آسـیب به شهرت مؤسسه و یا از دسـت دادن مزیت رقابتی آن شـود. در مقابل به نمایش‌گذاردن امنیت بالا در عملیات و امور مربوط به مشتریان، می‌تواند به یک مزیت رقابتی عمده تبدیل شـود. درنتیجه، توانایی بهره‌گیری از فناوری رقومی به‌صورتی ایمن به نقطه مرکزی موفقیت سـازمان بدل خواهد شد.

درحالی‌که ریسـک سـایبری بخشـی از دسـتور کار بسـیاری از هیئت‌مدیره‌ها شـده اسـت، این موضوع اغلب به‌اشـتباه به‌عنوان ریسـکی فنی که در حوزه اختیار مدیر ارشد اطلاعاتی می‌باشد، در نظر گرفته می‌شود. این باعث خوشـحالی است که هیئت‌مدیره‌ها بیشتر به موضوع ریسک سایبری توجه نشان می‌دهند. این علاقه به‌صورت سـؤالهای رو به افزایشـی که درباره موضوعهای سـایبر توسـط اعضای غیراجرایی هیئت‌مدیره از حسابرسـان می‌شـود، قابل‌لمس اسـت. بـا این حال، بسـیاری از مؤسسـه‌های تجاری تلاش می‌کنند تا آگاهی عمومی از مسـئله ریسکهای سایبری را به سمت فهم ریسـکهای مشخصی که گریبان‌گیر آنهاست و گامهای عملی مشخصی که در ارتباط با آن باید برداشته شود، سوق دهند.

هسـته مرکزی این مشـکل، در نظر گرفتن ریسـک سـایبری به‌عنوان موضوعی فنی می‌باشـد. چنین برداشتی این نکته مهم را که ریسـکهای سـایبری در اصل ریسـکهای تجاری هسـتند و اکثـر فعالیتهـای عملیاتـی و راهبردی شـرکت را تحت‌الشـعاع قـرار می‌دهند، نادیـده می‌انـگارد. چنین رویکردی رسـیدن به تصمیمهایـی را کـه بیـن فرصتها و ریسـکهای فنـاوری رقومی توازن ایجاد می‌کند، مشـکل می‌سـازد و اثر تجـاری عمده‌ای را که شکسـت امنیت سایبری می‌تواند به دنبال داشته باشد، نادیده می‌گیرد. به‌منظور مدیریت مؤثر ریسـک سایبری، مؤسسه‌های تجاری باید به آن به‌عنوان بخشی جدایی‌ناپذیر از راهبرد تجاری و عملیاتی خود و نه موضوعی فنی و تخصصی، نگاه کنند.

سـرمایه‌گذاران، مقررات‌گذاران و دیگر ذینفعان باید چگونگی ادغـام ریسـکهای سـایبری را در چارچـوب راهبـری کنونـی مدنظـر قـرار دهنـد. درحالی‌کـه هیئت‌مدیره‌هـا بایـد علاقه و مسـئولیت‌پذیری بیشـتری نسبت به ریسکهای سـایبری داشته باشند، ذینفعانی نظیر سرمایه‌گذاران و مقررات‌گذاران نیز باید این مسئله را مدنظر قرار دهند که چطور می‌توانند از توانایی یک بنگاه در حفاظت از اطلاعاتی که برای موفقیت آینده آن سرنوشت‌سـاز اسـت و همچنین مقاومت آن بنگاه در برابر حمله‌ها به زیربناهای رقومیش، مطمئن شوند.

کنترلهـا دربـاره امنیت اطلاعـات مالی برای سـالهای طولانی بخشـی از حسابرسی صورتهای مالی بوده اسـت. در هر صورت، موضوعهـای امنیت سـایبری گسـترده‌تر در چارچوب حسابرسـی صورتهـای مالـی قرار نمی‌گیرد؛ بلکه بخشـی از سـاختار راهبری گسـترده‌تر و از مسئولیتهای رعایت و مدیریت ریسک هیئت‌مدیره محسوب می‌شود. حسابرسان می‌توانند نقشی کلیدی در به چالش

اهمیت امنیت سایبری در سالهای اخیر به‌واسطه افزایش اتکا به فناوری اطلاعات و اینترنت رشد چشمگیری داشته است

کشیدن و یا اطمینان بخشیدن نسبت به مدیریت ریسکهای سایبری ایفا کنند. ذینفعان برون‌سازمانی نیز نیاز دارند که در نظر داشته باشند که چگونه بنگاه می‌تواند به‌طور معناداری این ریسکها را گزارش کند و سطح قابل قبولی از اطمینان را فراهم سازد.

گسترش رقومی شدن، باعث به‌وجود آمدن ریسک سیستمی در اقتصاد می‌شود که توجه دولتها به این بخش را توجیه می‌کند. تا به امروز اغلب دولتها تمام تمرکز خود را روی محافظت از داراییهای زیربنایی مهم ملی در برابر ریسکهای سایبری متمرکز کرده‌اند. در حالی‌که چنین تمرکزی صحیح بوده است، اما شاید بهتر باشد که دولتها علاقه خود را در زمینه ریسکهای سایبری به بحث اقتصاد نیز گسترش دهند. به‌عنوان مثال، اثر یک رویداد عمده در یک شرکت بزرگ یا در سرتاسر یک زنجیره تأمین، صرف‌نظر از اینکه آیا به‌عنوان یک دارایی زیربنایی مهم ملی طبقه‌بندی شده باشد یا خیر، می‌تواند آثار عمده‌ای بر اقتصاد داشته باشد. با توجه به درهم تنیده بودن اقتصاد، رویدادها می‌توانند به‌سرعت در زنجیره‌های تأمین گسترش پیدا کنند و این بدان معنی است که رویه‌های ضعیف در یک بنگاه می‌تواند دیگران را نیز در معرض خطر قرار دهد.

علاوه بر این، اگر قرار بر این است که مزایای فناوری رقومی را به حداکثر برسانیم و فعالیتهای اقتصادی بر پایه رقومی را گسترش دهیم، ایجاد اعتماد به فناوری رقومی در بین مؤسسه‌های تجاری و مشتریان ضروری است. امنیت باید در مرکز این اعتماد قرار گیرد؛ زیرا شکستهای امنیتی مستمر اعتماد عمومی را در معرض آسیب قرار می‌دهد. درنتیجه، دولتها علاقه قابل‌درکی برای اطمینان از این موضوع دارند که مؤسسه‌های تجاری با هر اندازه‌ای و در هر صنعتی به‌طور مؤثر به چالشهای مطرح‌شده در این گزارش واکنش نشان می‌دهند. این موضوع در علاقه رو به رشد دولتها در سرتاسر جهان برای گسترش رویه‌های امنیتی صحیح در کسب‌وکار، انعکاس یافته است.

با وجود این، عملکردهای دولتی در این حوزه به‌علت سرعت بالای تغییرات در فناوری و الگوهای تجاری و ابعاد بین‌المللی ذاتی ریسکهای تجاری، چندان مؤثر نبوده است؛ لذا چارچوبهای مقررات‌گذاری در این حوزه در عمل با مشکل مواجه بوده‌اند. علاوه بر این، پس از افشاگریهای **ادوارد اسنودن**[۶] (Edward Snowden) نیاز به ایجاد اعتماد مجدد به اعمال دولتها و اینکه آنها چگونه از اطلاعات حساس راجع به تهدیدها، نقاط آسیب‌پذیر و شکافهای امنیتی استفاده می‌کنند، حس می‌شود.

توصیه‌ها

- هیئت‌مدیره باید به دنبال شواهدی از همه بخشهای بنگاه در این ارتباط باشد که مدیران از ریسکهایی که فناوری رقومی برای راهبرد و عملیاتشان به همراه می‌آورد، آگاهی دارند و اقدامهای مناسبی را به‌منظور مدیریت این ریسکها در دستور کار دارند.
- مدیران غیراجرایی باید مدیران اجرایی را به چالش بکشند تا رویکردی منسجم در ارتباط با ریسکهای سایبری ارائه کنند.

خط‌مشی ۲: مؤسسه‌های تجاری باید بپذیرند که امنیت آنها در خطر خواهد بود

اگرچه خطرهای سایبری بسیار نامشخص باقی می‌ماند، اما گزارشهای رسانه‌ای، پژوهشهای صنعتی و تمام شواهد حاکی از رشد منابع احتمالی خطر و حجم شکافهای امنیتی است. گروه‌های سازمان‌یافته جنایی سایبری، جاسوسی‌های صنعتی دولتی، نفوذگران سیاسی و انفرادی، همه خطرهای بالقوه‌ای در مشاغل و کسب‌وکارها به حساب می‌آیند. خطرها و تهدیدهای داخلی هم به‌واسطه عملکرد کارمندان یا پیمانکاران بی‌دقت و بی‌انگیزه، همچنان قوی هستند.

مؤسسه‌های تجاری باید چابک باشند و بتوانند به‌سرعت در برابر انواع خطرهای سایبری واکنش نشان دهند

اطلاعات تجاری در زنجیره تأمین ارائه‌کنندگان خدمات به‌طور گسترده‌ای توزیع و پراکنده می‌شود. در سالهای اخیر، بسیاری از مؤسسه‌های تجاری نحوه عملکرد خود را از طریق استفاده از برون‌سپاری و پیمانکاران فرعی تغییر داده‌اند. در نتیجه، یک بنگاه اقتصادی بزرگ به‌طور معمول و به‌صورت مستقیم و غیرمستقیم، با هزاران عرضه‌کننده، ارائه‌کننده خدمات و پیمانکاران فرعی که اغلب در سرتاسر جهان تلاش و فعالیت می‌کنند، معامله خواهد کرد. شاید برخی از این عرضه‌کنندگان برای انجام مشاغل و حرفه خود، به اطلاعات تجاری ارزشمند و سری دسترسی داشته باشند. به‌عنوان مثال، پیمانکاران فرعی مهندسی می‌توانند به اموال و سرمایه‌های فکری دسترسی داشته باشند. آنها در کل می‌توانند به الگوهایی که برای پیشنهاد و مزایده برای شرکتها یا قراردادها آماده شده است، دسترسی داشته باشند. حسابداران نیز می‌توانند به اطلاعات مالی دسترسی داشته باشند.

با اینکه کار و فعالیت به این طریق می‌تواند از حیث کارایی، انعطاف‌پذیری و دسترسی به خدمات تخصصی ویژه مزایایی داشته باشد، اما **بنگاه توسعه‌یافته**[۷] چالشهای جدی و خطرناکی برای کنترل و امنیت اطلاعات ایجاد می‌کند. فرایندهای تدارکات باید با قراردادهایی که شرایط کنترل را تعیین می‌کند و دیگر روشهای ضمانتی، مسائل امنیت اطلاعاتی را مدنظر قرار دهند. هرچند، اغلب این فرض ضمنی وجود دارد که عرضه‌کنندگان روشهای خوبی را دنبال می‌کنند و تعداد کمی از قراردادها قوانین واضح و روشن کافی در این‌باره دارد. این مسئله با روشهایی مثل **رایانش ابری**[۸] بدتر خواهد شد؛ چون مؤسسه‌های تجاری باید به‌طور متناوب به شرایط و ضوابط عرضه‌کنندگان اتکا کرده و فرصت بسیار کمی برای تعیین شرایط و ضوابط خود و یا کسب ضمانت در خصوص کنترل و فرایندهای عرضه‌کنندگان خواهند داشت.

ابزار کاربری که در شبکه‌های شرکتی قرار دارند و اغلب با توجه به کارکرد مناسب و نه امنیت بالا طراحی شده‌اند، رشد و توسعه می‌یابد. کاربرد فراگیر و گسترده **کامپیوترهای کتابی**[۹] و تلفنهای هوشمند، عمومی شده است و کارمندان تقاضای دسترسی سیار به سیستمهای شرکتی را دارند. روش استفاده از **ابزار اختصاصی**[۱۰]، درجایی که کارمندان به‌جای استفاده از وسایل شرکت، از کامپیوترها، تلفنهای هوشمند و کامپیوترهای کتابی خود برای دسترسی به سیستمها و اطلاعات حرفه‌ای استفاده می‌کنند، در سالهای اخیر به‌سرعت رواج پیدا کرده است. در عین حال، این امر منتهی به از بین رفتن کنترل روی دستگاهها و اختلاط و ترکیب داده‌های شخصی و کاری در بسیاری از دستگاهها نیز شده است. همچنین، ابزار مجهز به اینترنتی در بسیاری از ابزار خانه‌داری هوشمند گرفته تا سیستمهای مدیریت موتور خودرو وجود دارند که می‌توانند برای ارسال و دریافت داده‌ها به شبکه‌های شرکت متصل شوند.

در بسیاری از این موارد، این دستگاه‌ها ارزان، یک‌بار مصرف و ساده طراحی می‌شوند. ایجاد امنیت بالا به‌طور معمول اولویت اصلی طراحان و تولیدکنندگان این ابزار کاربردی نیست و بنابراین باعث آسیب‌پذیری سازمان می‌شود.

مؤسسه‌های تجاری باید چابک باشند و بتوانند به‌سرعت در برابر انواع خطرهای سایبری واکنش نشان دهند. رقبا، خواه از منابع داخلی یا خارجی، می‌توانند در اقدامهای خود بسیار هدفمند، پیچیده و مقاوم باشند. به‌علاوه، بسیاری از وقایع و رویدادها می‌تواند ناشی از بی‌دقتی کارمندان باشد. مؤسسه‌های تجاری باید فرهنگ تجربه‌اندوزی از وقایع را ایجاد کنند و اعتماد ذینفعان را در هنگام بروز شکافهای امنیتی عمده حفظ کنند. با توجه به سرعت انتشار اخبار مربوط به شکافهای امنیتی که

از طریـق شـبکه‌های اجتماعی چـون **توئیتـر** (Twitter) در سرتاسـر جهان منتقل می‌شـود و تأثیر آن بر مشتریان، حفظ اعتماد ذینفعان اهمیت بالایی پیدا می‌کند.

رویه‌هـای جدیـد فناوری اطلاعـات به این مفهوم اسـت که مؤسسـه‌های تجاری همه باید بپذیرند که امنیت اطلاعاتی آنها بـه ناچار در خطر قرار می‌گیرد و این وضعیت مسـتلزم طرز فکر جدیـدی در حوزه امنیت اسـت. با اینکه مؤسسـه‌های تجاری باید همچنان کنترلهای پیشـگیرانه مناسـبی را به کار ببرند، اما نمی‌تواننـد انتظار داشـته باشـند که در تمام مکانهـا و در مقابل تمـام خطرهای احتمالـی، امنیت اطلاعات خـود را حفظ کنند. در عـوض، آنهـا باید به‌گونه‌ای عمل کنند که گویی امنیت‌شـان به‌خطر افتاده و برخی از اطلاعات آنها به دست افراد دیگر رسیده است. ما این وضعیت را **وضعیت خطر مفروض**[11] می‌نامیم.

تغییر فرهنگی عمده‌ای برای پذیرش این موضوع لازم است که شـکافهای امنیتی و هزینه اصلاح آنهـا و دیگر هزینه‌های مربوط، بخش جدایی‌ناپذیر انجام کار در محیط رقومی هستند؛ درست همانند **هزینه نقصان و آب‌رفتگی**[12] که ویژگی صنعت خرده‌فروشی است. با اینکه بنگاه‌های اقتصادی می‌توانند این هزینه‌هـا را کاهش دهند، اما ایـن هزینه‌ها به‌طور کامل حذف نخواهد شد.

وضعیـت خطر مفروض، مؤسسـه‌های تجاری را به سـمت همـکاری و تبـادل اطلاعات در خصوص خطرهای مشـترک بـا شـرکای مورد اعتمادشـان سـوق می‌دهد. ایـن موضوع با روشـهای سـنتی که بر لـزوم نگهـداری محرمانـه اطلاعات سیسـتمها به‌منظـور حفظ مزایای رقابتی یا ترس از آسـیب به اعتبار شـرکت تأکیـد دارد، مغایر اسـت. در چنین شـرایطی، رقبـا اغلب با هم همـکاری می‌کنند و اطلاعات را به اشـتراک می‌گذارند تا مانع وقوع حملات پیچیده شوند. درنتیجه، باید از پنهان‌کاری و فرهنگ دفاعی **نیاز به دانسـتن**[13]، به فرهنگ همـکاری بر مبنای **نیـاز به تبادل و اشـتراک‌گذاری**[14] تغییر جهت دهیم.

توصیه‌ها

• هیئت‌مدیـره باید بپذیرد که امنیت به‌خطر خواهد افتاد. برای انعکاس این خطر، گزارش هیئت‌مدیره باید بر تجربه‌اندوزی از وقایع خاص و آگاهی از میزان شـکافهای امنیتی که یک بنگاه خـاص آمادگی تحمـل آن را دارد، تمرکز کند. این امر حاکی از تغییر و تحول عمده‌ای در فرهنگ امنیت است.

• هیئت‌مدیـره بایـد در شبیه‌سـازیهای سـایبری از قبـل برنامه‌ریزی‌شـده و غیرمنتظـره شـرکت جسـته و از چنیـن برنامه‌هایـی حمایت کند. این مـوارد می‌تواند بـه فرایندهای تصمیم‌گیری در تمام سـطوح مؤسسـه و شناسایی نقاط ضعف بالقوه در توان پاسخگویی به تهدیدها مؤثر باشد.

خط‌مشـی ۳: مؤسسـه‌های تجـاری باید بـر دارایی‌های اطلاعاتی مهم خود تمرکز کنند

مؤسسـه‌های تجـاری نمی‌تواننـد از تمام سـرمایه اطلاعاتی خـود در تمام مـوارد محافظت کننـد؛ بلکه باید توجـه خود را بـه اطلاعات مهـم معطوف کنند. اغلب مؤسسـه‌های تجاری موقعیـت پیش‌فـرض حفظ و نگهـداری از همـه اطلاعات را برمی‌گزینند چون اولویت‌بنـدی و فیلتر دارایی‌های اطلاعاتی امری دشـوار و زمان‌بر است. با این حال، این رویکرد با توجه به رشد گسترده حجم اطلاعات که در اکثر مشاغل اتفاق افتاده اسـت و با توجه به تنوع بالای تهدیدهـای امنیتی و ضعفهای موجود، روزبه‌روز ناپایدارتر می‌شود.

در عوض، مؤسسه‌های تجاری باید سرمایه‌های اطلاعاتی خـود را اولویت‌بندی کنند و منابع خود را صرف اطلاعاتی کنند کـه در رقابـت و پایایی بنـگاه و موفقیت نهایی آن، بیشـترین اهمیت را دارا است.

این تغییر مسـتلزم پیشـرفت عمـده‌ای در درک دارایی‌های اطلاعاتی خواهد بود؛ چون امروزه تعداد کمی از مؤسسـه‌های تجـاری می‌توانند به‌سـادگی مهمترین اطلاعـات خود، محل ذخیره آنها و اینکه چه کسـی به آنها دسترسی دارد را شناسایی کنند. بنابراین مؤسسه‌های تجاری باید نظم بهتری ایجاد کنند و نسـبت به اولویت‌بندی انواع اطلاعات، دقت بیشتری به‌کار ببرند و تصمیمهای دشواری در خصوص اینکه کدام اطلاعات واقعاً مهم هستند، اتخاذ کنند.

بـا اولویت‌بنـدی سـرمایه‌های اطلاعاتـی، مؤسسـه‌های تجاری می‌توانند از رویکردی فنی درباره امنیت، به رویکردی مبتنی بر ریسـک تغییر جهت دهند. بسـیاری از مؤسسه‌های تجاری، امنیت را به‌عنوان یک مسـئله فنی در نظر می‌گیرند. اولویت‌بنـدی سـرمایه‌های اطلاعاتـی منتهی بـه رویکردی

می‌شود که مبتنی بر ریسک است و تصمیم‌گیری بهتری در خصوص توجیه کنترلهای خاص را میسر می‌کند.

به‌عنوان مثال، حائز اهمیت است که بدانیم تمامی کنترلها هزینه دارند و این هزینه‌ها شامل هزینه‌های مستقیم اجرای کنترل و هزینه فرصت مربوط به آهسته شدن و یا حتی توقف سایر فعالیتهای تجاری می‌شود. یک رویکرد مبتنی بر ریسک، امکان تصمیم‌گیری در خصوص متوازن کردن هزینه‌ها و منافع کنترلهای امنیتی را فراهم می‌کند. هنگامی‌که مؤسسه‌های تجاری به این تغییر و تحول دست یافتند و به کنترلها به‌عنوان خطر عملیاتی نگریستند، ممکن است تصمیم بگیرند که کنترلها را آسان‌تر کنند؛ البته درصورتی‌که این عمل به پاسخگو و مبتکر بودن آنها کمک کند.

با این حال، مدیریت امنیت به‌عنوان بخشی از خطر اجرایی و عملیاتی، نیاز به تعیین دقیق هزینه‌ها و منافع معیارهای امنیتی را ضروری می‌سازد. این اندازه‌گیری و ارزیابی، مشکلی پایدار در حوزه امنیت بوده است و قابلیتها در این زمینه باید رشد و توسعه پیدا کنند تا از تصمیم‌گیریهای پیچیده درباره کنترلهای خاص پشتیبانی کنند.

اولویت‌بندی دارایی‌های اطلاعاتی باید از طریق نظامهای مؤثر مالکیت بر اطلاعات و مسئولیت و پاسخگویی، پشتیبانی شود. این اولویت‌بندی تضمین می‌کند که تنها افراد خاصی انگیزه فعالیت و تصمیم‌گیری بر مبنای شواهد در خصوص استفاده و حفاظت از اطلاعات و برخورد با سؤالات گسترده‌تر کیفیت اطلاعاتی را دارند. بنابراین، ساختار راهبری قوی از رویکرد مبتنی بر خطر در مقوله امنیت حمایت و آن را تأیید می‌کند.

تعریف واضح و درست مالکیت اطلاعات حائز اهمیت است. تفاوت بین مسئولیت و پاسخگویی برای تضمین حفظ پاسخگویی در سطح بالاتر می‌تواند در اینجا مفید باشد و این در حالی است که مسئولیت امور جزئی به سطوح مناسب محول می‌شود.

مسئولیت اطلاعات خاص نیز باید به افراد مناسبی که نقش آن اطلاعات در بنگاه را می‌دانند و اختیار تصمیم‌گیری در خصوص حفاظت و کاربرد آن را دارند، محول شود. با اینکه این وظیفه گاهی به مدیران ارشد محول می‌شود، اما آنها اغلب نه آگاهی دقیق از امور جزئی و نه زمان لازم برای اتخاذ تصمیم مناسب در خصوص اطلاعات را دارند. به این ترتیب، در بسیاری از سازمانها مدیر ارشد اطلاعاتی به‌عنوان مالک اطلاعات در نظر گرفته می‌شود. با این حال، چنین رویکردی می‌تواند منجر به تأکید بی‌مورد بر ابعاد فنی شود. مالکیت اطلاعات باید بیشتر به افرادی که وظایف صفی دارند، محول شود.

توصیه‌ها

- هیئت‌مدیره باید از خود بپرسد که آیا می‌تواند سرمایه‌های اطلاعاتی مهم را شناسایی کند و آیا می‌داند که این اطلاعات کجا ذخیره می‌شوند و چه کسی به آنها دسترسی دارد. اگر پاسخ به این پرسشها واضح و روشن نیست، اعضای هیئت‌مدیره باید با مدیریت ارشد همکاری کنند تا درک صحیحی از داراییهای اطلاعاتی مهم و ریسکهای خاص مربوط به آنها به‌دست بیاورند.
- هیئت‌مدیره باید از اعمال سطوح مناسبی از مسئولیت و پاسخگویی به‌منظور پشتیبانی از اولویت‌بندی مؤثر داراییهای اطلاعاتی و تصمیم‌گیری مناسب در خصوص استفاده و حفاظت از اطلاعات مطمئن شود.

خط‌مشی ۴: اکثر مؤسسه‌های تجاری به حقوق اولیه و اساسی‌شان دست نمی‌یابند

براورد شده است که می‌توان بیش از ۸۰ درصد شکافهای امنیتی را با اجرای روشهای مقدماتی مناسب پیشگیری کرد. چنین روشهایی در بسیاری از موارد از جمله ابلاغیه سال ۲۰۱۲ **ده گام در امنیت سایبری**[۱۵] که به‌وسیله دولت انگلیس منتشر شد، تأکید شده و حاوی حفاظت به‌روز در برابر بدافزارها، دسترسی کنترل‌شده به سیستم و پشتیبان‌گیری منظم از آن است.

بدیهی است که مؤسسه‌های تجاری به‌سختی می‌توانند حقوق اولیه خود را در عمل به‌دست بیاورند. علاوه بر این، حسابرسان اغلب هرساله به این مشکلات و پیشرفت اندک حاصل‌شده در ارتباط با حل آن اشاره می‌کنند. با اینکه به‌طور معمول مدیریت قصد خوبی برای بهبود و توسعه دارد، اما این قصد به‌ندرت به عملکردی مؤثر تبدیل می‌شود.

دشواری در نیل به حقوق اولیه می‌تواند به عوامل مختلفی ارتباط داشته باشد. تجربه نشان می‌دهد که همه سازمانها با تمام اندازه‌ها و در تمام بخشهای صنعتی و بنا به دلایل متنوع،

هنـوز هم به دنبـال نیل به معیارهای اولیه هسـتند. سـرعت پیشـرفت فناوری و تغییرات تجاری به این معناست که عناصر کلیدی اولیه باید به‌صورت منظم و متناسـب با تغییر شـرایط، بازبینی و مرور شوند.

انـدازه و پیچیدگی محیـط فناوری اطلاعات در شـرکتهای بـزرگ، حتی مراحـل امنیتی اولیـه را در عمـل چالش‌برانگیز می‌کند. با رشـد و توسعه مؤسسه‌های تجاری، آنها ابزار بسیار و قطعات سـخت‌افزاری و نرم‌افزارهای کاربردی مختلفی را به هم متصل می‌کنند. سیسـتمها پس از سالها استفاده به‌صورت سفارشـی درآمده‌اند تا الزامهای محیط تجـاری در حال تغییر امـروزی را بـراورده سـازند. محیطهـای سیسـتمی پیچیـده می‌تواننـد با عدم هماهنگی و گوناگونی خدمات عرضه‌کنندگان فناوری اطلاعات، پیچیده‌تر شوند. در این شرایط، تنها به‌روز نگه‌داشتن نرم‌افزارهای ضدبدافزار و دیگر نرم‌افزارها می‌تواند بـرای مدیریـت پرهزینه، زمان‌بر و دشـوار باشـد. در گزارش بینـش حسابرسـی **انجمن حسـابداران خبره انگلسـتان و ولـز**[16] بـا عنوان «گـزارش بانکداری» به مسـائل ویـژه‌ای که شرکتهای بزرگ با آن مواجه هستند، پرداخته شده است.

در مقابل، دشواری رسیدن به حقوق اولیه در **مؤسسه‌های تجـاری بـا انـدازه کوچک‌ومتوسـط**[17] می‌توانـد بـه کمبود مهارت، منابع و اولویت‌بندی ارتباط داشته باشد. مؤسسه‌های تجـاری کوچک کمـی از کارمندان امنیتی متخصص اسـتفاده می‌کنند و احتمال دارد مدیریت در درک زبان فنی رایج در حوزه امنیت اطلاعات با مشـکل مواجه باشد. به‌علاوه، در بسیاری از مؤسسـه‌های تجاری با اندازه کوچک‌ومتوسط، موضوعهای اجرایی روزمره نسبت به معیارهای امنیتی اولویت پیدا می‌کنند و منتهی به سطح ضعیف‌تر و پایین‌تر امنیت می‌شوند.

افراد همچنان ضعیف‌ترین حلقه در اجرای معیارهای امنیتی اولیه هسـتند. اغلب نفوذها و شکافهای گسـترده درنهایت به خطا یا بی‌دقتی انسـانی ارتبـاط پیدا می‌کنـد. به‌عنوان مثال، کلیـک کـردن روی لینکهـای معیـوب و انتقـال ویـروس یـا بدافزارهـای دیگـر به درون سـازمان، رایج و متداول اسـت. اتصـال تجهیزات و دسـتگاه‌های خارجی معیوب، اسـتفاده از دسـتگاه تلفن همراه بدون امنیت مناسـب و یا اشتراک‌گذاری اطلاعات کاری در شبکه‌های اجتماعی، متداول شده است.

دغدغـه اجـرای معیارهای امنیتـی اولیه، برای بسـیاری از مؤسسـه‌های تجـاری به‌خصـوص مؤسسـه‌های تجـاری که گردش کارکنان بالا و قراردادهای متعددی دارند، فاصله زیادی تا برطرف شدن دارد. ایجاد فرهنگ هوشیاری دائمی نسبت به امنیت نیز در سـازمانی که کارمندان موقت دارد، دشـوار است. اطمینان از آموزش کافی کارمندان، بدون سـرمایه‌گذاری بیش از حد در زمان و منابع دیگر، ضروری است.

علاوه بر این، نگرش نسل جدید نسبت به فناوری با نگرش نسـل قبل تفاوت می‌کنـد. کارگران جدید راحت‌تـر از فناوری جدیـد اسـتفاده می‌کنند و اطلاعات را به اشـتراک می‌گذارند و می‌توانند فرصتها و مهارتهای جدیدی را وارد سـازمانها کنند. با این حال، گرایش و اشتیاق به فناوری نوین همیشه با میزان آگاهی از ریسکهای مرتبط با آن تطابق ندارد.

سازمانها باید پاسخگویی شخصی بیشتری در حوزه سیاستها و رویه‌هـای امنیتی ایجـاد کنند، تا افراد به‌تبـع آن رفتار خود را تغییر دهند. تشـویق افـراد به پیروی از روشـهای خوب به‌طور معمول چالشـی کلیـدی به همراه دارد و آن اینکه اغلب سـود و بهره شخصی کمی در این کار وجود دارد. در حقیقت، معیارهای امنیتـی روند انجـام کار را کند می‌کنـد و یا مانـع از انجام کار به روش دلخـواه کارمندان می‌شـود. تحقیقهای روان‌شناسـی به ما نشـان می‌دهد که افراد به‌طور معمـول در تصمیم‌گیری حول خطـر و موازنه مزایای کوتاه‌مدت در مقابل هزینه‌ها و ابهامهای بلندمدت، ضعیف هستند. لذا مؤسسه‌های تجاری باید مطمئن باشند که پیامدهای بی‌دقتی و رفتار نامناسب بدیهی است.

رویکردهای مختلفی در ارتباط با پاسخگویی می‌تواند اتخاذ شود. بنگاه‌های اقتصادی می‌توانند از روش «ابزار اختصاصی» برای ارتقای رفتار کارکنان اسـتفاده کننـد. زمانی که کارمندان

از وسایل خود استفاده می‌کنند، انگیزه بیشتری برای مراقبت صحیح از آنها پیدا می‌کنند. از طرف دیگر، زمانی که کارمندان نتوانند از دارایی‌ها به‌خوبی مراقبت کنند، مؤسسه‌های تجاری می‌توانند جرایم سخت‌گیرانه‌تری در مورد آنان اعمال کنند. زمانی که این جرائم به‌صورت صحیح و مؤثری اعمال شود، کاهش چشمگیری در تعداد وسایل و دستگاه‌های مفقودشده به‌وجود خواهد آمد.

مهارت‌های جدیدی برای پر کردن فاصله موجود بین امنیت و گستره تجارت لازم است. در بسیاری از بنگاه‌های اقتصادی، فاصله زیادی بین هیئت‌مدیره و عملکردهای امنیتی وجود دارد که در ارتباط مؤثر و درک مشترک از خطرها، مانع ایجاد می‌کند. در این شرایط، مؤسسه‌های تجاری به‌سختی می‌توانند در خصوص امنیت تصمیمهای مناسبی اتخاذ کنند و برای برقراری امنیت کافی، در مدیریت ارشد ایجاد تعهد نمایند.

رهبران امنیت اطلاعاتی باید به برقراری ارتباط با دیگر رهبران تجاری تمرکز کنند و فاصله بین هیئت‌مدیره و عملکرد امنیتی را از بین ببرند. یک مدیر ارشد امنیت اطلاعاتی با مهارتهای حرفه‌ای قوی می‌تواند این نقش را ایفا کند. در عمل، بسیاری از مؤسسه‌های تجاری پستهای به‌نسبت تخصصی مانند رئیس امنیت فناوری اطلاعات را به‌وجود می‌آورند.

به‌علاوه، آگاهی و مهارت بیشتری در خصوص امنیت سایبری برای مسئولیتهای تجاری موردنیاز است. اگر قرار است سایبر بخشی از **دی‌ان‌ای**[۱۸] یک بنگاه اقتصادی بشود، و نه اینکه فقط به متخصصان امنیت و فناوری اطلاعات واگذار شود، طیف گسترده‌ای از کارمندان باید در بحثهای مربوط به موضوعهای امنیتی مشارکت و آنها را درک نمایند.

توصیه‌ها

- هیئت‌مدیره باید از مسئولان فناوری اطلاعات و امنیت مؤسسه تجاری درباره میزانی که آنها به حقوق اولیه دست‌یافته‌اند، سؤال کند. توصیه‌های دولت و مشاوره از طرف اشخاص ثالث می‌تواند به هیئت‌مدیره کمک کند تا سؤالهای مناسبی برای پرسیدن را پیدا کند.
- هیئت‌مدیره باید تعهد قوی خود را نسبت به یک فرهنگ امنیتی قوی نشان دهد و رهبری خود را برای ایجاد تغییرات رفتاری در زمانی که به آن نیاز است، به نمایش بگذارد.

پانوشتها:

1- Cyber Security
2- Information Security
3- Supply Chain
4- Information Technology (IT)
5- Digital
۶- **ادوارد جوزف اسنودن**(Edward Snowden) متولد۲۱ ژوئن ۱۹۸۳ میلادی، افشاگر کنونی و کارمند سابق سازمان اطلاعات مرکزی آمریکا و پیمانکار سابق آژانس امنیت ملی است (ویکی‌پدیا).
7- Extended Enterprise
۸- **رایانش ابری** (Cloud Computing) مدل رایانشی بر پایه شبکه‌های رایانه‌ای مانند اینترنت است که الگویی تازه برای عرضه، مصرف و تحویل خدمات رایانشی (شامل زیرساخت، نرم‌افزار، بستر و سایر منابع رایانشی) با به کارگیری شبکه ارائه می‌کند (ویکی‌پدیا).
9- Tablets
10- Bring Your Own Device (BYOD)
11- An Assumed State of Compromise
12- Shrinkage Costs
13- Need to Know
14- Need to Share
15- Ten Steps to Cyber Security
16- The Institute of Chartered Accountants in England and Wales (ICAEW)
17- Small and Medium-Sized Enterprises (SMEs)
18- Deoxyribo Nucleic Acid (DNA)

منابع:

The Institute of Chartered Accountants in England and Wales (ICAEW), **Audit Insights Cyber Security**, icaew.com/auditinsights, 2013