نگرانیهای حسابرسان مستقل و ریسکهای امنیت سایبری

دکتر حلیمه رحمانی
روح‌اله آماره

ریسکهای امنیت سایبری

برای درک مفهوم ریسکهای سایبری باید ریشه‌ای به این موضوع نگاه کرد؛ جایی که **ایمنی**[۱]، رویدادهای تصادفی (مانند خرابی سرور) را پوشش می‌دهد در حالی که **امنیت**[۲] به موقعیتهای عمدی مربوط می‌شود (مانند حمله سایبری که توسط یک هکر انجام می‌شود). ایمنی با تهدیدهای داخلی سروکار دارد ولی هدف اصلی امنیت، برون‌سازمانی و خارجی است. بدون شک ایمنی با ریسک مرتبط است. ایمنی را می‌توان متضاد ریسک درنظر گرفت؛ به این معنی که وضعیت ریسک پایین و قابل‌قبول، ایمن شناخته می‌شود. با این توضیح نیز هیچ تعریف یکنواخت و پذیرفته‌شده‌ای از ریسک سایبری هنوز به اجماع همگان نرسیده است. ممکن است دلایل متعددی باعث این موضوع باشد و یکی از آن‌ها پیچیدگی در مفهوم است. ریسک سایبری یک موضوع میان‌رشته‌ای است که در بحثهای علمی تا آنجا که به تنوع ریسک سایبری و سرعت بسیار سریع تغییر در تهدیدهای سایبری و امنیت سایبری مربوط می‌شود، ظاهر شده است. مفهوم ریسکهای سایبری دارای دو جنبه فنی و اقتصادی است. از نظر فنی به اطلاعات و سیستمها برمی‌گردد، جایی که اطلاعات به شکل الکترونیکی در طول استفاده، پردازش، انتقال و ذخیره‌سازی استفاده می‌شوند، و سیستم به زیرساختها، نرم‌افزارها، افراد، فرایندها و داده‌هایی اطلاق می‌شود که برای کار با هم برای دستیابی به یک یا چند هدف خاص تجاری (برای مثال، ارائه خدمات یا تولید کالا) مطابق

با نظر مدیریت طراحی، پیاده‌سازی و بهره‌برداری می‌شوند. از نظر اقتصادی نیز به ارزیابی زیانها، ادعاها و بدهیهای احتمالی مربوط و ارزیابی تاثیر نهایی آن‌ها بر صورتهای مالی اشاره دارد. به‌صورت کلی ریسک سایبری شامل هرگونه ریسک ناشی از استفاده از فناوری اطلاعات و ارتباطات است که محرمانه‌بودن، دردسترس‌بودن یا یکپارچگی داده‌ها یا خدمات را به‌خطر می‌اندازد.

ریسکهای سایبری در نتیجه نقض امنیت اطلاعات شرکتها ایجاد می‌شوند و نقض امنیت اطلاعات در نتیجه حوادث امنیت سایبری رخ می‌دهند. حوادث امنیت سایبری به‌عنوان هر رویدادی که محرمانگی، یکپارچگی یا دردسترس‌بودن یک دارایی اطلاعاتی را به‌خطر می‌اندازد، تعریف می‌شود. به این ترتیب، حوادث امنیت سایبری ممکن است از انواع مختلفی از رویدادها مانند بدافزار، **باج‌افزار**[۳] یا حملات انکار سرویس، کلاهبرداری در پرداختهای کارتی، خودیهای مخرب یا حتی خطای انسانی تشکیل شود. حوادث امنیت سایبری رویدادهای پیچیده و چندوجهی هستند و پیامدهای کامل آن‌ها ممکن است همان لحظه محقق نشود. به همین خاطر شناسایی حوادث امنیت سایبری اغلب دشوار است و براورد تاثیر بالقوه آن‌ها، از نظر سوابق ازدست‌رفته یا سرقت‌شده و هزینه‌های مستقیم و غیرمستقیم مرتبط با آن، فرایند پیچیده‌ای است.

پیامدهای حوادث امنیت سایبری

در منطقه آمریکای شمالی، ایالات متحد همچنان در هزینه‌های حوادث امنیت سایبری در جهان پیشتاز است. میانگین هزینه‌ها در سال ۲۰۲۳ به ۹،۴۸ میلیون دلار رسید که بالاترین رقم در سطح جهان است. در اوایل سال ۲۰۲۴ نیز این رقم ۹،۳۶ میلیون دلار گزارش شد (IBM[۴]، ۲۰۲۴؛ CFO[۵]، ۲۰۲۴). این افزایش بر بار مالی فزاینده شرکتها تاکید می‌کند؛ زیرا آن‌ها با پیچیدگیهای تهدیدهای امنیت سایبری دست‌وپنجه نرم می‌کنند. کانادا همچنین افزایش هزینه‌های سایبری را تجربه کرد؛ جایی که میانگین آن به‌تقریب ۵،۱۳ میلیون دلار در سال ۲۰۲۳ براورد شد. این افزایش پیوسته نشان‌دهنده روندهای گسترده‌تری در چالشهای امنیت سایبری است که شرکتها در سراسر آمریکای شمالی با آن مواجه هستند (IBM 2024). در اروپا، آلمان میانگین هزینه نقض داده‌ها را ۴،۶۷ میلیون دلار در سال ۲۰۲۳ گزارش کرد (IBM 2024). این رقم چالشهای جاری شرکتهای اروپایی را در تامین امنیت اطلاعات حساس در برابر تهدیدهای سایبری نشان می‌دهد. علاوه‌بر این، منطقه بنلوکس، که شامل بلژیک، هلند و لوکزامبورگ می‌شود، از اوایل سال ۲۰۲۴ میانگین هزینه‌ای معادل ۵،۹ میلیون دلار گزارش کرد که نشان‌دهنده نگرانی فزاینده در مورد حوادث امنیت سایبری و پیامدهای مالی آن است (Statista 2024).

منطقه آسیا-اقیانوسیه به‌عنوان بیشترین هدف حمله‌های سایبری شناسایی شده که ۳۱٪ از کل حوادث گزارش‌شده را به‌خود اختصاص داده است (Cobalt 2024). در ژاپن، نقض اطلاعات به‌طور متوسط ۴،۵۲ میلیون دلار در سال ۲۰۲۳ بود (IBM 2024). در خاورمیانه نیز، متوسط هزینه نقض داده‌ها به‌طور قابل‌توجهی از ۶،۴۶ میلیون دلار در سال ۲۰۲۲ به ۸،۰۷ میلیون دلار در سال ۲۰۲۳ افزایش یافت که نشان‌دهنده نزدیک به ۲۰٪ افزایش است (IBM 2024). میانگین هزینه حوادث سایبری در خاورمیانه سالانه ۸،۴ درصد افزایش یافته و در سال ۲۰۲۴ به ۸،۷۵ میلیون دلار

یافته‌های اخیر

انجمن حسابرسان داخلی (IIA)

در سال ۲۰۲۳ نشان می‌دهد که

سازمانها به‌طور فزاینده‌ای نیاز به

کنترلهای داخلی قوی برای

کاهش ریسکهای امنیت سایبری را

تشخیص می‌دهند

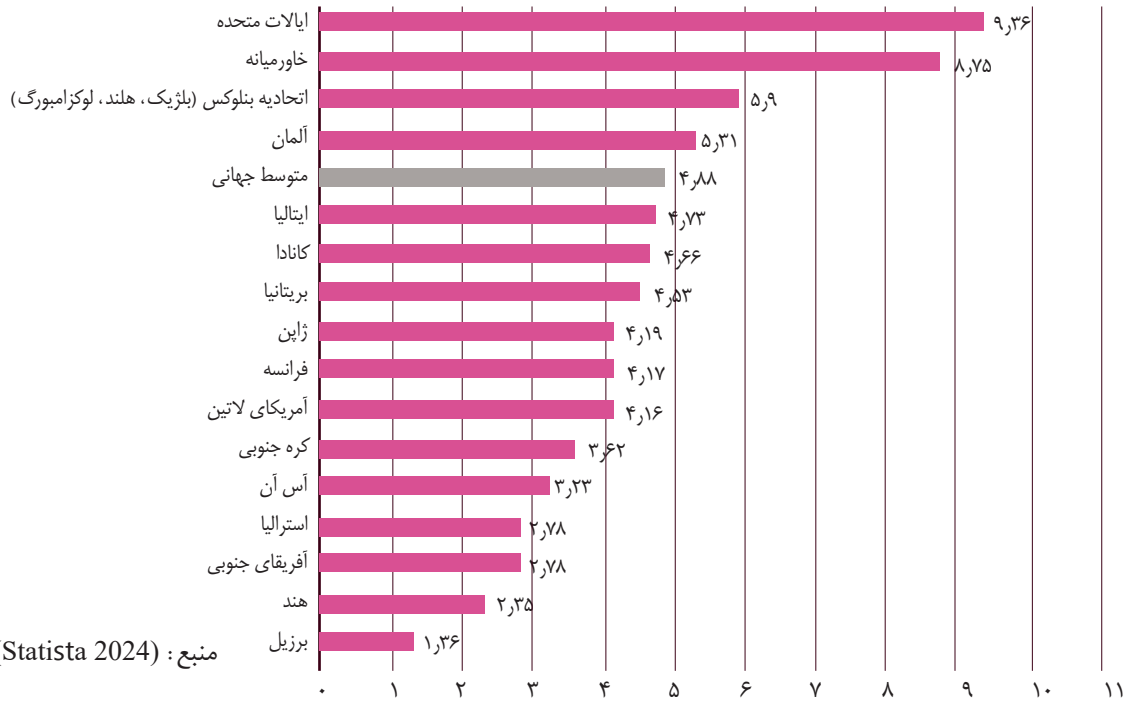
رسیده است. این رقم پس از ایالات متحد که میانگین هزینه آن ۹،۳۶ میلیون دلار گزارش شده است، جایگاه منطقه را به‌عنوان دومین منطقه برتر جهان حفظ می‌کند (**اخبار ملی**[۶]، ۲۰۲۴). در مقیاس جهانی، متوسط هزینه حوادث امنیت سایبری در سال ۲۰۲۴ به ۴،۸۸ میلیون دلار رسید و نسبت به ۴،۴۵ میلیون دلار در سال ۲۰۲۳ افزایش یافت (Statista 2024؛ Varoni 2024).

از کشورها و مناطق ذکرشده، ایالات متحد با میانگین هزینه سایبری ۹،۳۶ میلیون دلار، برای چهاردهمین سال پیشتاز هزینه‌ها بود. کانادا و ژاپن شاهد کاهش میانگین هزینه‌های سایبری در حالی بودند که ایتالیا و کشورهای خاورمیانه شاهد افزایش قابل‌توجهی بودند. منشا بیشتر حوادث امنیت سایبری به **حملات فیشینگ**[۷] (هکر با جعل هویت منابع معتبر، اقدام به فریب کاربران می‌کند و کاربران تصور می‌کنند در حال تعامل با یک منبع معتبر هستند) یا **حمله‌های اعتباری**[۸] (زمانی است که جزییات حساب شما توسط هکر (شامل نامهای کاربری، رمز عبور، پرسشهای امنیتی و سایر جزییات مخصوص فرد) برای جعل هویت و دسترسی به حسابها و سیستمها به‌سرقت می‌رود.) باز می‌گردد. نقض‌های ناشی از پیامهای فیشینگ ۴،۸۸ میلیون دلار هزینه دارند در حالی که اعتبارنامه‌های در معرض خطر ۴،۸۱ میلیون دلار هزینه دارند.

این روند صعودی مداوم در مناطق و صنایع مختلف، تاثیر مالی فزاینده حوادث امنیت سایبری در سراسر جهان را برجسته می‌کند. میانگین هزینه‌ها در صنعت مراقبتهای بهداشتی سال ۲۰۲۳ به ۱۰،۹۳ میلیون دلار رسید و پس از آن خدمات مالی در حدود ۵،۹ میلیون دلار قرار دارند (IBM 2024). صنعت مراقبتهای بهداشتی با میانگین هزینه ۹،۷۷ میلیون دلار در سال ۲۰۲۴، در صدر همه صنایع قرار گرفت -که از سال ۲۰۱۱ تاکنون پیشرو بوده است. صنعتی که بیشترین افزایش در هزینه‌های سایبری را داشته است، که میانگین افزایش هزینه ۸۳۰،۰۰۰ دلاری به‌ازای هر حادثه را تجربه کرده است.

پیش‌بینی می‌شود که جرایم سایبری در سال ۲۰۲۴ به‌تقریب ۹،۵ تریلیون دلار برای جهان هزینه داشته باشد و انتظار می‌رود تا سال ۲۰۲۵ به ۱۰،۵ تریلیون دلار در سال افزایش یابد (Statista 2024). این پیش‌بینی هشداردهنده بر

نمودار ۱: میانگین هزینه حوادث امنیت سایبری از مارس ۲۰۲۳ تا فوریه ۲۰۲۴، براساس کشور یا منطقه (به میلیون دلار)



منبع: (Statista 2024)

نیاز فوری به استراتژیهای امنیت سایبری قوی در تمام قاره‌ها تاکید می‌کند. حملات فیشینگ همچنان رایج است؛ به‌ویژه در آمریکای شمالی، جایی که تنها در طول سال ۲۰۲۳ منجر به نزدیک به ۲۰ میلیارد دلار خسارت شده است (CFO 2024). این داده‌ها نه‌تنها تاثیر مالی حوادث امنیت سایبری را نشان می‌دهد، بلکه نیاز روزافزون شرکتها در سراسر قاره‌ها را برای سرمایه‌گذاری در اقدامها و استراتژیهای جامع امنیت سایبری برای کاهش موثر این هزینه‌های فزاینده نشان می‌دهد.

نگرانی حسابرسان مستقل درباره ریسکهای سایبری

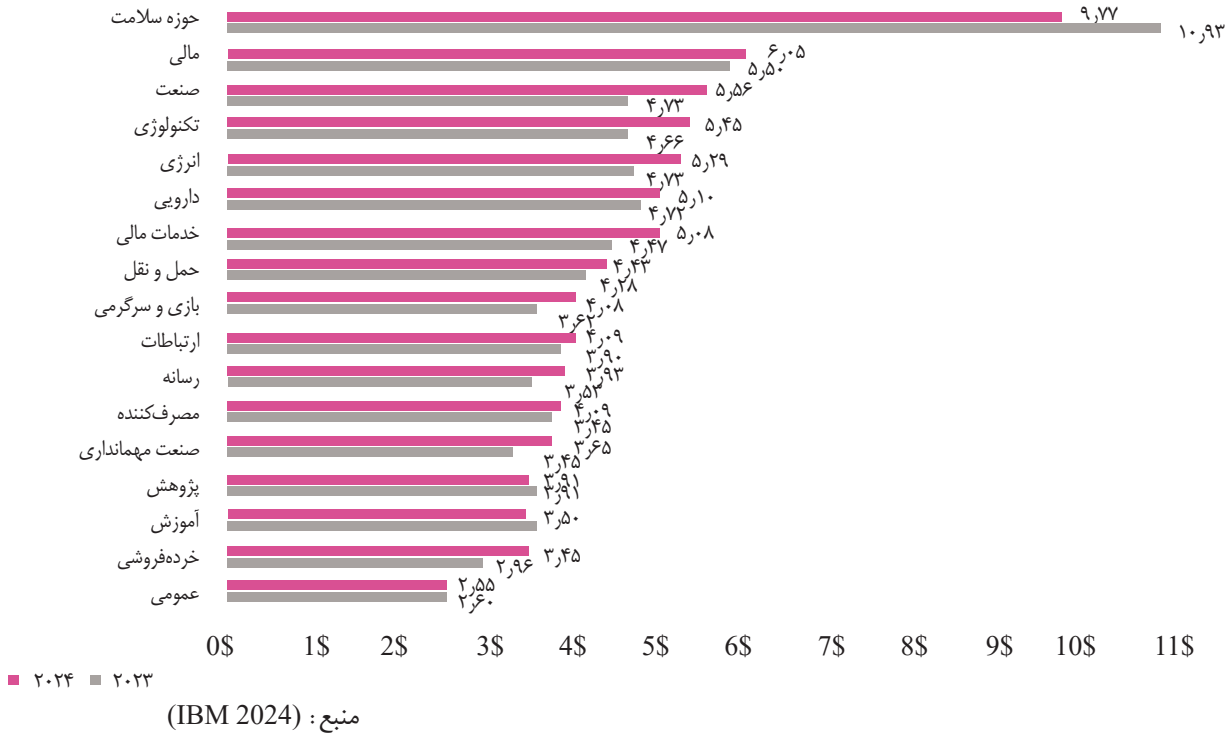
حسابرسان مستقل دلایل متعددی برای نگرانی در مورد ریسکهای سایبری دارند، که تحت عناوین فرعی زیر بحث می‌شود:

الف- پیامدهای ریسک سایبری: زمانی که یک حادثه امنیت سایبری رخ می‌دهد، حسابرسان مستقل مسئول ارزیابی زیانها، ادعاها و بدهیهای مربوط به ریسکهای سایبری مشتری و ارزیابی تاثیر نهایی آن بر صورتهای مالی هستند. به‌طوری‌که شرکتهایی که از حوادث امنیت سایبری رنج می‌برند، با هزینه‌های مستقیم (هزینه‌های اصلاح، هزینه‌های قانونی، جریمه‌ها و تراکنشهای از دست رفته) و غیرمستقیم (از دست‌دادن درامدهای فعلی و آتی و همچنین زوال اعتماد صاحبکار و جامعه که براورد چنین هزینه‌هایی بنا به تعریف دشوار است). متعدد و غیرمنتظره‌ای مواجه می‌شوند.

طبق گزارش سالانه IBM در مورد حوادث امنیت سایبری، میانگین هزینه حوادث امنیت سایبری در سال ۲۰۲۴ به ۴،۸۸ میلیون دلار افزایش یافته که نشان‌دهنده افزایش ۱۰ درصدی نسبت به سال قبل است. این افزایش نشان‌دهنده بزرگترین جهش از زمان همه‌گیری کرونا است و به افزایش هزینه‌های مرتبط با ازدست‌دادن کسب‌وکار، خرابیهای عملیاتی و واکنشهای پس از حوادث نسبت داده می‌شود. همچنین بیش از ۴۵ درصد این حوادث سایبری مربوط به اطلاعات شخصی مشتریان است، در حالی که ۴۳ درصد شامل سوابق سرمایه‌های فکری "ایده‌ها" است.

ب- ضعف کنترلهای داخلی: حوادث امنیت سایبری

نمودار ۲: میانگین هزینه حوادث امنیت سایبری براساس صنایع مختلف (به میلیون دلار)

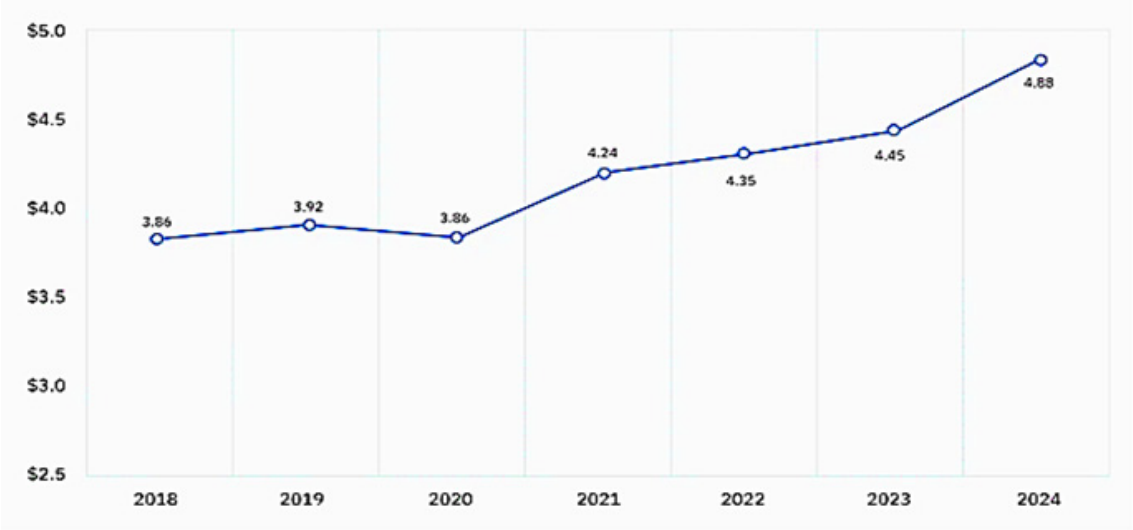


منبع: (IBM 2024)

همچنین ممکن است نشانه‌ای از ضعفهای بالقوه در رابطه با کنترل داخلی بر گزارشهای مالی (کنترل داخلی حاکم بر گزارشگری مالی) باشد. ریسک امنیت سایبری می‌تواند به شکل ضعفهای کنترلی(ضعفهای کنترل فناوری اطلاعات) و یا به‌عنوان نقاط ضعف در گزارشگری مالی تحقق یابد. استاندارد شماره ۳۱۵ حسابرسی ایران و استاندارد شماره ۱۲ **هیئت نظارت بر حسابداری شرکتهای سهامی عام**[۹] (PCAOB) به‌صراحت حسابرسان را ملزم می‌کنند که باید شناختی از نحوه استفاده شرکتها از فناوری اطلاعات (IT) و تاثیر فناوری اطلاعات بر صورتهای مالی به‌دست آورند. به این ترتیب، حسابرسان مستقل باید نقاط قوت و ضعف فناوری اطلاعات شرکتها را به‌دقت ارزیابی و درک کنند و آن‌ها را در ارزیابی ریسک خود بگنجانند. یافته‌های اخیر **انجمن حسابرسان داخلی**[۱۰] (IIA) در سال ۲۰۲۳ نشان می‌دهد که سازمانها به‌طور فزاینده‌ای نیاز به کنترلهای داخلی قوی برای کاهش ریسکهای امنیت سایبری را تشخیص می‌دهند، به‌طوری که ۶۰ درصد از رهبران حسابرسی داخلی گزارش داده‌اند که از زمان شروع همه‌گیری، تمرکز خود را بر کنترلهای فناوری اطلاعات افزایش داده‌اند (IIA 2023). علاوه‌براین، **هیئت استانداردهای بین‌المللی حسابرسی و اعتباربخشی**[۱۱] (IAASB) استانداردهای خود را به‌روز کرده است تا بر اهمیت ارزیابی ریسکهای مربوط به امنیت سایبری تاکید کند، به‌ویژه در پرتو تهدیدهای در حال تحول که می‌تواند یکپارچگی مالی را به‌خطر بیندازد (IAASB 2023). بنابراین حسابرسان باید رویکردی پیشگیرانه در ارزیابی این خطرها اتخاذ کنند تا از نظارت جامع و کنترلهای داخلی موثر اطمینان حاصل شود.

ت- نهادهای نظارتی و استانداردگذاران: حسابرسان مستقل تحت فشار فزاینده‌ای از سوی نهادهای نظارتی و استانداردگذاران در رابطه با امنیت سایبری هستند. به‌عنوان مثال، **مرکز کیفیت حسابرسی**[۱۲] (CAQ)، بارها بر این واقعیت تاکید کرده است که حسابرسان باید توجه خاصی به این نوع حوادث داشته باشند (CAQ 2014. 2016. 2017. 2019). به‌ویژه در شرایطی که نهادهای نظارتی بر تهدیدهای سایبری نظارت را شدت بخشیدند. در یک نظرسنجی مشترک اخیر با دیلویت، امنیت سایبری به‌عنوان اولویت اصلی کمیته‌های حسابرسی ظاهر شد، به‌طوری که ۶۹ درصد از پاسخ‌دهندگان آن را به‌عنوان یکی از نگرانیهای اصلی برای سال آینده برجسته کردند، و ۳۰ درصد آن را به‌عنوان اولویت اول خود رتبه‌بندی می‌کنند که بسیار بیشتر از سایر موضوعها مانند مدیریت ریسک سازمانی است (Deloitte & CAQ 2023). همچنین از حسابداران رسمی (CPA) حمایت می‌کند تا با استفاده از مهارت خود در مدیریت ریسک و

نمودار ۳: میانگین جهانی هزینه حوادث امنیت سایبری (به میلیون دلار)



منبع: (IBM 2024)

ارزیابیهای مستقل، نقشی اساسی در افزایش انعطاف‌پذیری امنیت سایبری ایفا کنند (CAQ 2023). این تمرکز افزایش یافته بیشتر ناشی از الزامهای افشای جدید از سوی کمیسیون بورس و اوراق بهادار ایالات متحد (SEC) است که شرکتها را موظف می‌کند که خطرها و حوادث امنیت سایبری را گزارش کنند؛ بنابراین نظارت بیشتر کمیته‌های حسابرسی را ضروری می‌کند (SEC 2022). در همین راستا، **کمیسیون بورس و اوراق بهادار آمریکا**[۱۳] (SEC) نیز الزامهای افشای خود را در رابطه با ریسکهای سایبری را افزایش داده است. اکنون چنین ریسکی باید به‌صراحت در صورتهای مالی لحاظ شود (SEC 2011. 2014. 2018). علاوه بر این، در سایر کشورها نیز ارزیابی ملی تهدیدهای سایبری ۲۰۲۳-۲۰۲۴ نشان می‌دهد که جرایم سایبری، به‌ویژه باج‌افزار، مهم‌ترین تهدید برای سازمانهای کانادایی باقی می‌ماند و بر نیاز به اقدامهای امنیت سایبری قوی در سراسر بخشها تاکید می‌کند (**ایمنی عمومی کانادا**[۱۴]، ۲۰۲۳). در نهایت، گزارش هیئت نظارت بر حسابداری شرکتهای عام دوباره تاکید کرد که ریسک سایبری حتی اگر بر کنترل داخلی حاکم بر گزارشگری مالی تاثیری نداشته باشد، باقی می‌ماند؛ چراکه آسیب‌پذیریهای بالقوه آتی را نشان می‌دهد (PCAOB 2010).

نتیجه‌گیری

حوادث امنیت سایبری چالشهای مهمی را برای حسابرسان مستقل و همچنین نگرانیهای جدی در مورد یکپارچگی گزارشگری مالی و کنترلهای داخلی ایجاد کرده است. همانطور که این حوادث بیشتر و پیچیده‌تر می‌شوند، اغلب نشان‌دهنده ضعفهای اساسی در سیستمهای کنترل داخلی یک شرکت، به‌ویژه در کنترلهای **فناوری اطلاعات** (IT) هستند. پیچیدگی روزافزون تهدیدهای سایبری ایجاب می‌کند که حسابرسان هوشیار باشند؛ زیرا حوادث امنیت سایبری می‌تواند منجر به زیانهای عملیاتی قابل‌توجه، افزایش تلاشهای حسابرسی و هزینه‌های بالاتر مرتبط با خطرهای دادرسی ناشی از حاکمیت ضعیف شود. از آنجایی که حق‌الزحمه حسابرسی ارتباط نزدیکی با میزان کار مورد نیاز و خطرهای مرتبط با آن، ازجمله خطر دادرسی دارد، حسابرسان ممکن است برای کاهش ادعاهای قانونی احتمالی ناشی از حوادث سایبری، دریافت حق بیمه را درنظر بگیرند. با همه این توضیحها و هزینه‌های گزاف در نتیجه ریسک سایبری، هنوز رهنمود جامعی نسبت به این مسایل از سوی نهادهای ناظر یا استانداردگذاران صورت نگرفته است. فقدان رهنمودهای روشن از سوی نهادهای نظارتی بر نیاز به تحقیق و توسعه بیشتر در این زمینه تاکید می‌کند. فارغ از این موضوع، این مطالعه کمکهای متعددی به ادبیات موجود می‌کند و ارتباط بین نگرانیهای حسابرسان مستقل و ریسک سایبری و تا حدودی نگرانیهای استانداردگذاران در مورد مسایل امنیت سایبری با حسابرسان مستقل را به‌خوبی نشان می‌دهد. در نهایت، از آنجایی که سازمانها به‌طور فزاینده‌ای به زیرساختهای دیجیتال متکی هستند، حسابرسان باید اقدامهای پیشگیرانه‌ای را در ارزیابی ریسکهای امنیت سایبری اتخاذ کنند تا از یکپارچگی مالی و اعتماد عمومی خدمات خود اطمینان حاصل کنند.

پانوشتها:

1- Safety
2- Security
3- Ransomware
4- International Business Machines Corporation (IBM)
5- Chief Financial Officer (CFO)
6- The National News
7- Phishing Attacks
8- Compromised Credential Attack
9- Public Company Accounting Oversight Board (PCAOB)
10 Institute of Internal Auditors (IIA)
11- International Auditing and Assurance Standards Board (IAASB)
12- Center for Audit Quality (CAQ)
13- Securities and Exchange Commission (SEC)
14- Public Safety Canada (PSC)

منابع:

- Center for Audit Quality - CAQ. (2024). Audit Committee Practices Report. https://www.thecaq.org/audit-committee-practices-report-2024
- Statista Inc. (2024). Global Average Cost of a Data Breach by Country. Retrieved from https://www.statista.com/statistics/463714/cost-data-breach-by-country-or-region/