پنج راهبرد برای مبارزه با تقلب

Annie Hylton
Sarah Ovaska

با گسترش و پیچیده‌تر شدن جرایم اقتصادی در سراسر جهان، کاهش تهدید روزافزون مستلزم سرمایه‌گذاری درخورتوجه و کنترلهای موثر است.

بر اساس گزارش رخنه در داده‌ها منتشرشده به‌وسیله موسسه **پونمون** (Ponemon)، متوسط هزینه جهانی رخنه در داده‌ها در سال ۲۰۱۹ نزدیک به ۳/۹۲ میلیون دلار بود، که نسبت به سال ۲۰۱۸ حدود ۱/۵درصد رشد داشته است.

همه‌گیری کووید۱۹، کشف تقلب را بسیار ضروری‌تر ساخته است؛ زیرا با محدودیت جریانهای نقدی در شرکتها در مفهوم کوچک و بزرگ، این روزها حتی قدرت کمتری برای جبران زیان غیرمنتظره وجود دارد.

نایجل آیر (Nigel Iyer)، کارشناس در زمینه تقلب، ساکن کشورهای نروژ و بریتانیا و شریک موسسه **بی‌فور اینوستیگیت** (B4 Investigate) و یکی از بنیانگذاران **آموزشگاه تقلب** (Fraud Academy) و همچنین همکار و حسابدار رسمی در **انجمن حسابداران خبره مدیریت** (CIMA)، بر این باور است که سارقان خبره نیز به تلاش خود برای سرقت پول در محیط آشفته جهانی که همه‌گیری مسبب آن بود، شدت داده‌اند.

آیر معتقد است که امروز با وجود کاهش درخورتوجه تجارت فرامرزی و دیگر درهم‌ریختگیهای موجود در سازمانهای مجرمانه، "*مجرمان به‌واقع پراکنده شده‌اند. شما به نرخ جرایم سایبری نگاه کنید که روندی روبه‌رشد دارد.*"

هرچه زمان شناسایی و کشف رخنه در داده‌ها در یک سازمان طولانی‌تر شود، هزینه آن بیشتر می‌شود. در سال ۲۰۱۹، چرخه زندگی برای رخنه در داده‌ها ۲۷۹ روز بود و بیش از نیمی از موارد رخنه در داده‌ها در سال ۲۰۱۹ ناشی از حمله‌های مخرب و جنایتکارانه بود. بر اساس گزارش موسسه پونمون، دیگر موارد، ناشی از نقص فنی سیستم و خطای انسانی بودند.

اما آماده‌سازی، به‌معنای واقعی و صوری کلمه نتیجه می‌دهد.

بر اساس نظرسنجی انجام‌شده از بیش از ۵۰۰۰ مدیر اجرایی موسسه **پرایس‌واترهاوس‌کوپرز** (PwC) با موضوع نظرسنجی تقلب و جرایم اقتصادی جهانی ۲۰۲۰، موسسه‌هایی که برنامه‌هایی را برای تقلب درنظر گرفته‌بودند، ۴۲ درصد کمتر با حوادث واقعی تقلب مواجه شده‌بودند و نسبت به موسسه‌هایی که در این زمینه، برنامه‌هایی درنظر نگرفته‌بودند، ۱۷ درصد کمتر هزینه‌های اصلاحی داشتند. این نظرسنجی همچنین نشان داد که نزدیک به ۴۰ درصد از پاسخ‌دهندگان گفتند که قصد دارند به‌منظور پیشگیری از تقلب در دو سال آینده هزینه‌ها را افزایش دهند.

به نکته‌های زیر برای سرمایه‌گذاری بالا در زمینه مبارزه با تقلب توجه کنید. مدیران مالی به‌ویژه می‌توانند در سال جاری به آنها بپردازند.

ارزیابی ریسک

هنوز بسیاری از سازمانها به پیشگیری از تقلب به‌عنوان رویکردی واکنشی و دفاعی می‌پردازند. بر اساس گزارش پرایس‌واترهاوس‌کوپرز، تقریبا نیمی از سازمانهای جهانی ارزیابی ریسک را انجام نمی‌دهند، یا تنها یک ارزیابی غیررسمی انجام می‌دهند.

اما به گفته **ژولز کلبورن بابر** (Jules Colborne Baber)، شریک موسسه **دیلویت** (Deloitte) و مدیر جرایم اقتصادی مستقر در لندن، شرکتها باید اقدام پیشگیرانه‌ای را برای جلوگیری از تقلب انجام دهند و اولین گام در این راه، ارزیابی ریسک تقلب است.

کلبورن بابر گفت که ارزیابی مناسب ریسک تقلب که دامنه کامل فعالیتهای سازمان را در بر می‌گیرد، این امکان را برای شرکتها فراهم می‌آورد که خطرهای ناشی از آن را شناسایی و سپس کنترلها را بر اساس این خطرها طراحی کنند. شما باید منشا خطرها را شناسایی کنید؛ به‌همین ترتیب می‌توانید بر اساس منشا آن، چارچوب مدیریت ریسک تقلب خود را توسعه دهید. افزون بر این، باید ببینید افراد شایسته‌ای برای نظارت و اطمینان از آن چارچوب و بررسی موارد اشتباه وجود دارد یا خیر.

طبق ارزیابی کلبورن بابر، بهترین ارزیابیها با استفاده از داده‌های کمی و کیفی انجام می‌شود و می‌توان از کارگاه‌ها یا نظرسنجیها برای گرداوری داده‌ها استفاده کرد. ریسکهای ذاتی ارزیابی می‌شوند و به‌طور معمول محورهای احتمالی و بااهمیت و سپس کنترلها شناسایی و برای مقابله با ریسکها طراحی می‌شوند، تا ریسک باقیمانده به‌دست آید. با تغییر کسب‌وکار و محیط آن، ارزیابی نیز باید به‌طور مستمر به‌روز شود.

به گفته کلبورن بابر، شرکتها می‌توانند به روشهای مختلف به سرمایه‌گذاری در ریسک و ارزیابی آن بپردازند، اما به‌طور معمول این سرمایه‌گذاری توسط رده دوم با مشارکت رده اول کسب‌وکار هدایت می‌شود. کسب‌وکارها می‌توانند ارزیابی را به‌طور داخلی انجام دهند یا مشاوران خارجی استخدام کنند. نکته اصلی از نظر وی این است که این مسئله یک تلاش همگانی است. هزینه چنین ارزیابیهایی به مقیاس و ماهیت کسب‌وکار بستگی دارد.

آموزش آگاهی از تقلب

باید میان آموزش و برقراری ارتباط با کارکنان در مورد فرهنگ سازمانی، سیاستهای داخلی منع فعالیتهای متقلبانه و علائم هشداردهنده و ریسکهای تقلب سازگاری برقرار باشد. برنامه‌های گزارشگری تقلب باید اجرا و در اختیار کارکنان قرار گیرد.

به گفته موسسه پرایس‌واترهاوس‌کوپرز، این سازگاری باید سیاست داخلی و خارجی برای فروشندگان در داخل و خارج را دربر گیرد تا بتواند به عنوان یک سیستم هشداردهنده اولیه در مورد مشکلات احتمالی سازمان عمل کند.

ریکاردو نورنا (Ricardo Norena)، شریک اصلی اروپای غربی در موسسه **یی‌وای** (EY)، مستقر در مادرید گفت: "*ایجاد آگاهی در برابر تقلب و مبارزه با فساد در سازمان بسیار اهمیت دارد.*"

نورنا توصیه می‌کند که نشستهای آموزشی به‌احتمال به‌عنوان بخشی از نشستهای شرکت برگزار گردد، و اصول سازمانی و بایدها و نبایدها به اطلاع عموم افراد رسانده شود. آموزش در زمینه پیشگیری از تقلب برای کارکنان جدید انجام شود.

نورنا می‌گوید: "*در بیشتر موارد تقلب به ما ثابت می‌کند که آگاهی کافی در سازمان وجود نداشته است.*"

ایر اشاره کرد که هدف اصلی، جذابیت بخشیدن به این آموزشها است. تعداد زیادی از شرکتها به ارائه اطلاعات در طول سمینارهای بی‌نتیجه و بدون تلاش زیاد برای اطمینان از جلب توجه و جذب کارکنان بسنده کرده‌اند. او گفت که این نشستهای آموزشی غیرالهام‌بخش، شانس انتقال پیام را کاهش می‌دهد و کارکنان در واقع از روشهای ضروری برای پیشگیری و توقف تقلب استفاده می‌کنند. ایر گفت: "*باید کشف تقلب را به یک سرگرمی تبدیل کنید.*" او بر این باور است که موفقیت‌آمیزترین آموزش، بازی کشف تقلب است که در آن حسابداران و دیگران می‌توانند نقش کارآگاهان کشف تقلب را ایفا کنند.

افراد توانمندشده

در بیشتر اوقات، کارکنان بزرگترین وسیله دفاعی یک شرکت در

برابر تقلب هستند. به‌نظر ایر بسیاری از طرحهای تقلب توسط کارکنان باهوش در بخش مالی یا دیگر بخشها کشف می‌شوند که متوجه می‌شوند به‌نظر چیزهایی نادرست هستند. به‌همین دلیل، مدیر باید اطمینان حاصل کند که به‌طور منظم و مداوم پیامهایی مبنی‌بر ضرورت بررسی و گزارش رفتار و عوامل مشکوک تامین‌کنندگان وجود دارد. او نسبت به اتکای بیش از حد به فناوری برای جلوگیری از تقلب هشدار داد و پیشنهاد کرد که شرکتها بر این تمرکز کنند که چگونه کارکنان درگیر این موضوع، اولین کسانی هستند که نمایشنامه‌های مشکوک را تشخیص می‌دهند. ایر گفت: «*در واقع فرایندی وجود ندارد که تقلب را کشف کند، خود افراد این کار را انجام می‌دهند.*»

این موضوع، چالشی برای نیروهای کار از راه‌دور طی مدت همه‌گیری کووید ۱۹ است؛ شما نمی‌توانید به دفتر همکاران خود وارد شوید و از آنها بخواهید به یک صورتحساب یا سفارش خرید عجیب نگاه کنند. ایر گفت: "*برای مردم اغلب راحتتر است که به میز کار کسی سربزنند و بگویند: این کمی عجیب است؛ نظر شما چیست؟*"

تحلیل‌گری داده‌ها

به‌طور تاریخی، سازمانها به تقلب در صورت وقوع واکنش نشان می‌دهند و سپس محیط کنترلی خود را بهبود می‌دهند. کلبورن بابر می‌گوید اما شرکتها باید به‌طور روزافزون به رویکرد فعالتری روی آورند و این رویکرد، استفاده از تحلیل‌گری داده‌ها در کل فرایند مدیریت ریسک تقلب است. تحلیلگری داده‌ها می‌تواند برای شناسایی نقاط ضعف کنترل یا تشخیص ناهنجاریهایی که می‌توانند شاخص تقلب باشند، استفاده شود.

وی گفت: "*مسئله مهم برای من ابزار تحلیلگری داده‌ها برای نظارت است. ما شاهد سرمایه‌گذاری کسب‌وکارها در زمینه نظارت بر فعالیتهای مربوط به اتلاف، خلافکاری و تقلب هستیم.*"به‌عنوان نمونه، این حوزه‌ها می‌توانند هزینه تدارک و استخدام کارکنان در راستای شناسایی و پیشگیری از مشکلات و ارتقای فرایندها را شامل شوند. این گونه‌ای از قابلیتهای تحلیلی است که شامل نگهداری و تبدیل داده‌ها، استفاده از روشهای پیچیده تحلیلگری و تصویرسازی این نتایج در پیشخوان به‌منظور بررسی و پیگیری است.

هزینه سرمایه‌گذاری با توجه به ماهیت سازمان بسیار متفاوت خواهد بود؛ اما به گفته کلبورن بابر، نکته اصلی برای هر سازمان این است که برای نشان‌دادن ارزش کار از یک آزمایش اولیه یا اثبات ایده شروع کند و سپس از آنجا اقدام کند.

کنترلهای مبارزه با تقلب

سازمانها باید در جهت ایجاد کنترلهای داخلی قویتر که فرصت ارتکاب تقلب را مورد هدف قرار می‌دهند، هزینه کنند. بر اساس نظرسنجی موسسه پرایس‌واترهاوس‌کوپرز، از هر ده شرکت، کمتر از سه شرکت آزمون محدودی در مورد اثربخشی عملکرد کنترلهای خود انجام می‌دهند و ۱۲ درصد دیگر نیز هیچ آزمونی انجام نمی‌دهند.

از دیدگاه نورنا ، چنین کنترلهایی شامل سرمایه‌گذاری در فناوری و اقدام متمرکز بر مردم است. سرمایه‌گذاری در کنترل فناوری، نه‌تنها در فناوری، بلکه همه کنترلهای پیرامون فناوری بااهمیت هستند.

سازمانها همچنین باید بر کنترلهایی که موجب نادیده‌گرفتن یا تبانی با مدیریت می‌شوند، سرمایه‌گذاری کنند. نورنا می‌گوید از آنجا که کنترلهای داخلی می‌توانند توسط کارکنان یا اشخاص ثالث دستکاری شوند، وجود کارشناسان مستقل برای پیشگیری از بستگی در سازمان الزامی است. تفکیک وظایف، مستندسازی تراکنشها، چرخش شغلی، و مرخصی اجباری برای ایجاد مانع در برابر کلاهبرداران در کنترل انحصاری دفاتر، نمونه‌هایی از کنترلهای احتمالی است. این کنترلها باید به‌طور یکنواخت از نظر اثربخشی مورد نظارت قرار گیرند و به‌دنبال پیشرفت در فناوری، به‌روزرسانی شوند.

حسابداران مدیریت با تشویق موسسه‌های خود برای اقدام در جهت سرمایه‌گذاری برای کشف و پیشگیری از تقلب، می‌توانند به سازمانهای خود در جهت کاهش و پیشگیری از زیانهای بعدی، کمک کنند.

منبع:

. Hylton A, Ovaska S., **5 Strategies for Investing in Anti-fraud Efforts**, September 2020