

مدیریت ریسک و ارزش در امنیت سایبری سازمانی

محمدامین صادقی^۱، حسین کارگر^۲، مهدی اکبری دهزیری^۳، علی مصلی نژاد^۴

^۱ باشگاه پژوهشگران جوان و نخبگان، واحد جهرم، دانشگاه آزاد اسلامی، جهرم، ایران

^۲ گروه مهندسی برق واحد جهرم، دانشگاه آزاد اسلامی، جهرم، ایران

^۳ گروه مهندسی برق واحد جهرم، دانشگاه آزاد اسلامی، جهرم، ایران

^۴ دپارتمان مهندسی فناوری اطلاعات، دانشگاه آزاد اسلامی، واحد الکترونیک، تهران، ایران

چکیده

مدیریت ریسک را می‌توان فرآیندی برای حفظ دارایی‌ها، قدرت و امنیت دانست و مهندسی ارزش، مدیریت ارزش بخشی جدایی ناپذیر از مدیریت ریسک به حساب می‌آید. یکپارچه سازی مهندسی ارزش و مدیریت ریسک باعث ایجاد هم افزایی می‌شود؛ این هم افزایی وقتی در امنیت سایبری پیاده شود، می‌تواند بر امنیت سایبری تاثیر بگذارد. این مقاله ارزیابی ریسک امنیت سایبری مبتنی بر ارزش، درجه تاثیر و درجه سختی بررسی می‌کند. در این پژوهش با هدف کسب نظر خبرگان درباره ریسک های امنیت اطلاعات سازمانی پرسشنامه بین خبرگان توزیع شد، از میان عوامل امنیت اطلاعات ۵۵ ریسک امنیتی استخراج شد که سرانجام در قالب ۱۵ ریسک امنیتی مشخص شد. در این پرسشنامه، هر یک از خبرگان که تعداد آنها ۱۰ نفر بود نظر خود را درباره میزان ریسک تک تک عوامل برای امنیت اطلاعات در طیف پنج گانه لیکرت از طریق متغیرهای کلامی (خیلی کم، کم، متوسط، زیاد و خیلی زیاد) و با رویکردی مدیریت ارزش ابراز کردند. درجه تاثیر هزینه هر ریسک و سختی آن برای سازمان مشخص شد. در این مطالعه که مطالعه تطبیقی بین ریسک ها از نظر ارزش آن ها برای سازمان بود، یافته ها نشان داد عملکرد توأم مدیریت ریسک و مهندسی ارزش در امنیت، با افزایش امنیت همراه خواهد بود بوده است.

واژه‌های کلیدی: امنیت سایبر، ارزیابی ریسک امنیتی، مدیریت ریسک، ارزش