

حملات سایبری از نظر پیچیدگی و بزرگی و نیز توانایی تخریب آنها به سرعت در حال افزایش است. استفاده از مدیریت ریسک امنیت سایبری به منظور مدیریت این تهدیدها برای سازمان‌ها ضروری است. با این وجود، چارچوب‌های فعلی دارای اشکالاتی است که می‌تواند منجر به تخصیص غیربهبینه منابع امنیت سایبری شود. بیمه سایبری به عنوان یک راه حل برای مدیریت ریسک و امنیت سایبری مطرح است. بر اساس این ایده، بیمه‌گران می‌توانند با ارائه تخفیف‌های مناسب در حق بیمه، شرکت‌ها را برای بهبود امنیت سایبری خود تشویق کنند. اما سطح پذیرش بیمه‌های سایبری همچنان پائین است. دلیل این امر این است که شرکت‌ها در تعیین اینکه کدام محصولات بیمه سایبری را خریداری می‌کنند با مشکل روبرو هستند. شرکت‌های بیمه نیز برای ارزیابی دقیق ریسک سایبری و در نتیجه تولید محصولات بیمه سایبری همچنان تلاش می‌کنند. برای مقابله با این چالش‌ها، کتاب حاضر، مدل‌های جدیدی را برای مدیریت ریسک امنیت سایبری ارائه می‌دهد که بخشی از آن براساس استفاده از بیمه سایبری است. در این کتاب، مباحث زیر ارائه شده است:

- مجموعه‌ای از مدل‌های ریاضی برای مدیریت ریسک امنیت سایبری، از جمله (الف) الگویی برای کمک به شرکت‌ها در تعیین تخصیص بودجه بهینه خود بین محصولات امنیتی و بیمه سایبری و (ب) الگویی برای کمک به بیمه‌گران در طراحی محصولات بیمه سایبری.
 - استفاده از مدل‌هایی برای تجزیه و تحلیل ریسک برای گزارش رفتار عوامل تهدیدآمیز و همچنین رفتار شرکت‌ها و بیمه‌ها.
- شایان ذکر است که برای آگاهی از این مدل‌ها، از مطالعات تصمیم‌گیری سازمانی و نیز مطالعات اقتصاد رفتاری و روانشناسی برای تصمیم‌گیری توسط افراد در مورد امنیت سایبری و بیمه سایبری استفاده شده است. یافته‌های نظری و روش‌شناختی این کتاب، برای پژوهشگران در طیف وسیعی از رشته‌های مرتبط با امنیت سایبری از جمله تجزیه و تحلیل ریسک و تصمیم‌گیری، مدیریت فناوری، علوم اکچوئری، علوم رفتاری و اقتصاد مفید است. از سوی دیگر، یافته‌های عملی به متخصصان و بیمه‌گران امنیت سایبری کمک می‌کند تا امنیت سایبری و بیمه سایبری را افزایش دهند. این کتاب در ۱۴۸ صفحه و ۶ فصل به نگارش درآمده است.



نویسنده:

David Rios Insua
Caroline Baylon
Jose Vila

ناشر:

Chapman and Hall/CRC

سال نشر:

۲۰۲۱

شابک:

9780367339494