

امنیت سائبری

ریسک و تاب آوری

مؤلفین

کارول الف. سیگل

مارک سوینی

مترجم

دکتر ایوب ترکیان

نیاز دانش

Siegel, Carol A	: سیگل، کارول ا.	سرشناسه
: امنیت سایبری: ریسک و تاب‌آوری / مولف کارول الف. سیگل، مارک سوینی؛ مترجم ایوب ترکیان.	: عنوان و نام پدیدآور	
: تهران: نیاز دانش، ۱۳۹۹.	: مشخصات نشر	
: ۱۸۳ ص: مصور (بخشی رنگی)، جدول.	: مشخصات ظاهری	
: 978-600-8906-95-7	: شابک	
: فیبا	: وضعیت فهرست نویسی	
: عنوان اصلی: Cyber strategy : risk-driven security and resiliency , 2020	: یادداشت	
: کامپیوترها -- ایمنی اطلاعات	: موضوع	
: شبکه‌های کامپیوتری -- تدابیر ایمنی	: موضوع	
: سوینی، مارک	: شناسه افزوده	
: ترکیان، ایوب، ۱۳۳۷ - مترجم	: شناسه افزوده	
: QAV۶/۹	: رده بندی کنگره	
: ۰۰۵/۸	: رده بندی دیویی	
: ۷۴۰۱۸۹۰	: شماره کتابشناسی ملی	
: فیبا	: وضعیت رکورد	



www.ketab.ir

: امنیت سایبری، ریسک و تاب‌آوری	: نام کتاب
: کارول الف. سیگل، مارک سوینی	: مؤلفین
: دکتر ایوب ترکیان	: مترجم
: حمیدرضا محمد شیرازی - محمد شمس	: مدیر اجرایی - ناظر بر چاپ
: نیاز دانش	: ناشر
: واحد تولید انتشارات نیازدانش	: صفحه‌آرا
: سوم - ۱۴۰۰	: نوبت چاپ
: ۵۰ نسخه	: شمارگان
: ۷۰۰۰۰۰ ریال	: قیمت

ISBN:978-600-8906-95-7

شابک: ۹۷۸-۶۰۰-۸۹۰۶-۹۵-۷

هرگونه چاپ و تکثیر (اعم از زیراکس، بازنویسی، ضبط کامپیوتری و تهیهی CD) از محتویات این اثر بدون اجازه کتبی ناشر ممنوع است. متخلفان به موجب بند ۵ از ماده ۲ قانون حمایت از مؤلفان، مصنفان و هنرمندان تحت پیگرد قانونی قرار می‌گیرند. کلیه حقوق این اثر برای ناشر محفوظ است.

آدرس انتشارات: تهران، میدان انقلاب، خیابان ۱۲ فروردین، تقاطع وحید نظری، پلاک ۲۵۵، طبقه ۱، واحد ۲

۰۲۱-۶۶۴۷۸۱۰۶-۶۶۴۷۸۱۰۸-۰۹۱۲۷۰۷۳۹۳۵

www.Niaze-Danesh.com

مشاوره جهت نشر: ۰۹۱۲ - ۲۱۰۶۷۰۹

فهرست مطالب

۱۱	فصل اول: ضرورت امنیت سایبری
۱۲	۱-۱ تبیین رویکرد
۱۲	۲-۱ گام‌های توسعه راهبرد
۱۳	۳-۱ بازیگران اصلی راهبرد
۱۴	۴-۱ تدوین راهبرد
۱۵	۵-۱ عوامل محرکه تهیه راهبرد
۱۵	۶-۱ امنیت اطلاعات و امنیت سایبری
۱۵	۱-۶-۱ امنیت اطلاعات
۱۶	۲-۶-۱ امنیت سایبری
۱۷	۷-۱ تاب‌آوری سایبری و تاب‌آوری سنتی
۱۹	۸-۱ چرخه حیات راهبرد
۲۰	۹-۱ راهبردها و برنامه‌های سایبری
۲۱	۱۰-۱ برنامه سازمانی امنیت و تاب‌آوری سایبری
۲۲	۱۱-۱ معماری: استانداردها و چارچوب‌ها
۲۳	۱-۱۱-۱ معماری امنیت اطلاعات سازمانی
۲۴	۲-۱۱-۱ معماری امنیت مقرراتی
۲۴	۳-۱۱-۱ مقدمه چارچوب امنیت سایبری NIST (CSF)
۲۶	۱۲-۱ پیش‌برنامه‌ریزی سایبری
۲۷	۱۳-۱ جوانب فنی تمرکز برنامه سایبری
۲۹	فصل دوم: گام‌های تدوین و نگهداری راهبرد
۲۹	۱-۲ گام ۱: آمادگی برای توسعه راهبرد
۲۹	۱-۱-۲ فرهنگ شرکت و تحلیل سازمانی
۳۱	۲-۱-۲ ساختار سازمانی ماتریسی
۳۲	۳-۱-۲ ساختار سازمانی سیلویی
۳۳	۴-۱-۲ توانمندسازی سازمان برای اقتباس راهبرد
۳۴	۵-۱-۲ تشکیل کمیته راهبری
۳۵	۶-۱-۲ عوامل موفقیت تدوین برنامه راهبردی
۳۵	۷-۱-۲ انتصاب مدیر پروژه کمیته راهبری
۳۶	۸-۱-۲ تدوین فعالیت‌های کمیته راهبری

- ۹-۱-۲ استقرار ارزش‌های سازمان ۳۶
- ۱۰-۱-۲ تعیین رسالت/نگرش، اصول، و اهداف راهبردی ۳۶
- ۱-۱۰-۱-۲ رسالت/نگرش ۳۷
- ۲-۱۰-۱-۲ اصول برنامه سایبری ۳۸
- ۳-۱۰-۱-۲ اهداف راهبردی ۳۸
- ۲-۲ گام ۲: مدیریت پروژه راهبردی ۳۹
- ۱-۲-۲ اقدامات برای اهداف امنیت سایبری راهبردی ۳۹
- ۲-۲-۲ اقدامات برای اهداف راهبردی تاب‌آوری سایبری ۴۲
- ۳-۲-۲ تدوین منشور پروژه راهبردی ۴۳
- ۴-۲-۲ ترازبندی راهبرد با دیگر راهبردها و اهداف ۴۵
- ۵-۲-۲ تهیه شابلون گزارش‌دهی کلان برنامه راهبردی ۴۶
- ۶-۲-۲ تعیین تلاش‌های کاری ۴۶
- ۷-۲-۲ مسیر زمانی راهبرد ۴۷
- ۸-۲-۲ مسیر حرکت راهبرد ۴۸
- ۹-۲-۲ نگاشت اقدام NIST CSF ۴۹
- ۱۰-۲-۲ سند نهایی راهبرد ۴۹
- ۳-۳ گام ۳: تهدیدات، آسیب‌پذیری‌ها، و تحلیل اطلاعاتی ۵۰
- ۱-۳-۲ تهدیدات سایبری ۵۰
- ۱-۱-۳-۲ گزارش‌دهی ریسک تهدید سایبری ۵۱
- ۲-۳-۲ اطلاعات، شناسایی، و مدل‌سازی تهدید ۵۱
- ۳-۳-۲ آسیب‌پذیری‌ها ۵۱
- ۱-۳-۳-۲ آسیب‌پذیری‌های مربوط به دارایی‌ها ۵۱
- ۲-۳-۳-۲ گزارش‌دهی ریسک شدت آسیب‌پذیری ۵۲
- ۴-۲ گام ۴: ریسک‌ها و کنترل سایبری ۵۲
- ۱-۴-۲ تعاریف رده ریسک سایبری برای کسب و کار ۵۲
- ۲-۴-۲ استعداد ریسک و تحمل ریسک ۵۳
- ۳-۴-۲ روش‌شناسی‌های سنجش ریسک سایبری ۵۳
- ۱-۳-۴-۲ مدیریت ریسک سایبری ۵۳
- ۱-۱-۳-۴-۲ چارچوب مدیریت ریسک سایبری NIST ۵۴
- ۲-۳-۴-۲ محاسبه ریسک سایبری ۵۵
- ۴-۴-۲ کنترل‌ها ۵۶
- ۵-۴-۲ بیمه سایبری ۵۷
- ۵-۲ گام ۵: ارزیابی حالات فعلی و هدف ۵۷

۵۸	۱-۵-۲ انواع ارزیابی‌ها
۵۹	۶-۲ گام ۶: سنجش عملکرد
۶۰	۱-۶-۲ شاخص‌های ریسک و عملکرد سایبری
۶۱	۷-۲ چرخه‌ها و فرایندهای حکمرانی
۶۲	۸-۲ پیشنهاد اقدامات جدید کاهش تهدیدات و کاهش ریسک
۶۲	۱-۸-۲ نمونه گزارش سالیانه امنیت و تاب‌آوری سایبری
۶۳	۲-۸-۲ تدقیق راهبرد با گذشت زمان - اقدامات آخر سال
۶۳	۱-۲-۸-۲ جمع‌آوری داده‌ها برای سنجش عملکرد راهبرد
۶۴	۲-۲-۸-۲ تدوین گزارش سالیانه عملکرد
۶۴	۳-۲-۸-۲ تعیین اقدامات جدید برای سال بعد
۶۴	۴-۲-۸-۲ انجام فعالیت‌های مختلف مدیریت پروژه
۶۵	۹-۲ چک‌لیست‌ها و شابلون‌ها
۶۷	فصل سوم: مدیریت پروژه سایبری
۶۷	۱-۳ نگرش جریان اقدامات
۶۸	۲-۳ منشور پروژه راهبرد
۶۸	۳-۳ چک‌لیست آماده‌سازی راهبرد
۷۰	۴-۳ مسیر زمانی راهبرد
۷۱	۵-۳ چارت گانت راهبرد
۷۱	۶-۳ خط مسیر راهبرد
۷۲	۷-۳ دیاگرام‌های جریان داده
۷۵	۸-۳ ماتریس تدوین راهبرد RACI
۷۵	۹-۳ نقشه اقدام NIST CSF
۸۲	۱۰-۳ گزارش نهایی راهبرد
۸۵	فصل چهارم: تهدیدات، آسیب‌پذیری‌ها، و تحلیل اطلاعات سایبری
۸۶	۱-۴ تهدید در فضای راهبرد سایبری
۸۷	۱-۱-۴ تعریف تهدید
۸۷	۲-۱-۴ تکامل تهدیدات سایبری
۸۷	۱-۲-۱-۴ مراحل اولیه
۸۸	۲-۲-۱-۴ بازیگران تهدید فعلی و آتی
۸۹	۳-۱-۴ انواع تهدیدات و بازیگران
۹۰	۱-۳-۱-۴ هکرهای آماتور
۹۰	۲-۳-۱-۴ هکرهای حرفه‌ای
۹۱	۳-۳-۱-۴ گروه‌های جرایم سازمان‌یافته

- ۹۱..... ۴-۳-۱-۴ بازیگران دولت پایه
- ۹۲..... ۵-۳-۱-۴ تهدیدات داخلی
- ۹۳..... ۶-۳-۱-۴ تهدیدات مبتنی بر هوش مصنوعی
- ۹۳..... ۴-۱-۴ اطلاعات، شناسایی، و مدل سازی تهدید
- ۹۴..... MITRE ATT&CK ۱-۴-۱-۴
- ۹۵..... ۲-۴-۱-۴ جایگاه در داخل راهبرد و برنامه
- ۹۶..... ۳-۴-۱-۴ پایش تهدیدات
- ۹۶..... ۴-۴-۱-۴ گزارش اطلاعات تهدید
- ۹۷..... ۱-۴-۴-۱-۴ مرتبط کردن اطلاعات تهدید به هیئت مدیره
- ۹۸..... ۲-۴ آسیب پذیری ها
- ۹۸..... ۱-۲-۴ پروژه امنیت اپ وب باز (OWASP)
- ۱۰۰..... ۲-۲-۴ شناسایی آسیب پذیری ها
- ۱۰۱..... ۱-۲-۲-۴ موضوعات مدیریت آسیب پذیری نوین
- ۱۰۱..... ۳-۲-۴ آسیب پذیری های موبوط به دارایی
- ۱۰۲..... ۴-۲-۴ سیستم رتبه بندی آسیب پذیری رایج (CVSS)
- ۱۰۴..... ۵-۲-۴ آسیب پذیری ها در فضای راهبرد
- ۱۰۵..... ۳-۴ حملات سایبری
- ۱۰۵..... ۱-۳-۴ انواع رایج
- ۱۰۶..... ۲-۳-۴ انواع ائتلاف معمول
- ۱۰۹..... فصل پنجم: ریسک ها و کنترل های سایبری
- ۱۰۹..... ۱-۵ ریسک سایبری
- ۱۰۹..... ۱-۱-۵ چارچوب ریسک سایبری
- ۱۱۰..... ۲-۱-۵ تعاریف رده ریسک
- ۱۱۲..... ۳-۱-۵ تحمل ریسک و استعداد ریسک
- ۱۱۲..... ۱-۳-۱-۵ استعداد ریسک
- ۱۱۳..... ۲-۳-۱-۵ تحمل ریسک
- ۱۱۳..... ۳-۳-۱-۵ تفاوت تحمل و استعداد
- ۱۱۳..... ۴-۱-۵ روش شناسی سنجش ریسک سایبری
- ۱۱۴..... ۱-۴-۱-۵ مستند ۳۰-۸۰۰
- ۱۱۵..... ۵-۱-۵ نمونه ارزیابی ریسک سایبری ۳۰-۸۰۰
- ۱۱۹..... ۱-۵-۱-۵ توصیف ریسک NIST برای سازمان های دولتی
- ۱۱۹..... ۲-۵-۱-۵ رتبه بندی تهدید تقابلی NIST
- ۱۱۹..... ۶-۱-۵ دیگر روش شناسی های ارزیابی ریسک سایبری

۱۱۹	۱-۶-۱-۵ چارچوب ریسک ISACA- ریسک IT
۱۲۰	۲-۶-۱-۵ ISO/IEC سری ۲۷۰۰۰
۱۲۱	۳-۶-۱-۵ راهنمای PMBOK
۱۲۲	۴-۶-۱-۵ روش‌شناسی رتبه‌بندی ریسک OWASP
۱۲۳	۵-۶-۱-۵ COSO ERM
۱۲۴	۶-۶-۱-۵ آنالیز فاکتور ریسک اطلاعات (FAIR)
۱۲۴	۱-۶-۶-۱-۵ نمونه FAIR
۱۲۴	۲-۶-۶-۱-۵ مدل مدیریت ریسک FAIR
۱۲۶	۷-۶-۱-۵ روش کمی‌سازی ریسک CM RQM
۱۲۷	۱-۷-۶-۱-۵ شاخص ریسک
۱۲۷	۷-۱-۵ افشای ریسک
۱۲۸	۲-۵ کنترل‌های IT
۱۲۸	۱-۲-۵ وظایف اصلی کنترل‌ها
۱۲۹	۲-۲-۵ رشدیافتگی کنترل‌ها
۱۳۰	۳-۲-۵ مرکز امنیت اینترنت کنترل‌های امنیت اصلی
۱۳۰	۴-۲-۵ ممیزی کنترل‌های فناوری اطلاعات
۱۳۰	۳-۵ بیمه سایبری
۱۳۲	۱-۳-۵ انتقال ریسک
۱۳۵	فصل ششم: ارزیابی‌های حالت فعلی و هدف
۱۳۵	۱-۶ مقدمه ارزیابی‌ها
۱۳۶	۲-۶ ارزیابی‌های حالت فعلی
۱۳۷	۱-۲-۶ رده‌های ارزیابی‌ها
۱۳۷	۱-۱-۲-۶ خودارزیابی‌ها
۱۴۰	۲-۱-۲-۶ ارزیابی‌های بیرونی
۱۴۱	۳-۱-۲-۶ ممیزی (داخلی و خارجی)
۱۴۱	۲-۲-۶ چارچوب‌ها، استانداردها، مقررات، و مدل‌ها
۱۴۱	۱-۲-۲-۶ شناساگرها و رده‌های اصلی
۱۴۱	۳-۶ انجام ارزیابی حالت فعلی
۱۴۹	۴-۶ بحث اقدامات نگاشت نشده
۱۵۱	۵-۶ ارزیابی حالت هدف
۱۵۲	۱-۵-۶ حالات هدف NIST CSF
۱۵۳	۶-۶ نحوه درجه‌بندی حالات فعلی و هدف