

# امنیت سایبری

## ریسک و تاب آوری

مؤلفین

کارول الف. سیگل

مارک سوینی

مترجم

دکتر ایوب ترکیان

نیاز دانش

## 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.....

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

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	..... <b>فصل سوم: مدیریت پروژه سایبری</b>
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	..... <b>فصل چهارم: تهدیدات، آسیب‌پذیری‌ها، و تحلیل اطلاعات سایبری</b>
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

- ۹۱-۴-۱-۳ بازگران دولت پایه.....
- ۹۲-۴-۱-۳ تهدیدات داخلی.....
- ۹۲-۴-۱-۳ تهدیدات مبتنی بر هوش مصنوعی.....
- ۹۳-۴-۱-۳ اطلاعات، شناسایی، و مدل‌سازی تهدید.....
- ۹۴-۴-۱-۳ MITRE ATT&CK.....
- ۹۵-۴-۱-۳ جایگاه در داخل راهبرد و برنامه.....
- ۹۶-۴-۱-۳ پایش تهدیدات.....
- ۹۶-۴-۱-۳ گزارش اطلاعات تهدید.....
- ۹۷-۴-۱-۳ مرتبط کردن اطلاعات تهدید به هیئت مدیره.....
- ۹۸-۴-۲ آسیب‌پذیری‌ها.....
- ۹۸-۴-۲-۱ پروژه امنیت اپ وب باز (OWASP).....
- ۱۰۰-۴-۲-۲ شناسایی آسیب‌پذیری‌ها.....
- ۱۰۱-۴-۲-۲ موضوعات مدیریت آسیب‌پذیری نوین.....
- ۱۰۱-۴-۲-۳ آسیب‌پذیری‌های مربوط به دارایی.....
- ۱۰۲-۴-۲-۴ سیستم رتبه‌بندی آسیب‌پذیری رایج (CVSS).....
- ۱۰۴-۴-۲-۵ آسیب‌پذیری‌ها در فضای راهبرد.....
- ۱۰۵-۴-۳ حملات سایبری.....
- ۱۰۵-۴-۳-۱ انواع رایج.....
- ۱۰۶-۴-۳-۲ انواع ائتلاف معمول.....
- ۱۰۹- فصل پنجم: ریسک‌ها و کنترل‌های سایبری.....**
- ۱۰۹-۵-۱ ریسک سایبری.....
- ۱۰۹-۵-۱-۱ چارچوب ریسک سایبری.....
- ۱۱۰-۵-۱-۲ تعاریف رده ریسک.....
- ۱۱۲-۵-۱-۳ تحمل ریسک و استعداد ریسک.....
- ۱۱۲-۵-۱-۳-۱ استعداد ریسک.....
- ۱۱۳-۵-۱-۳-۲ تحمل ریسک.....
- ۱۱۳-۵-۱-۳-۳ تفاوت تحمل و استعداد.....
- ۱۱۳-۵-۱-۴ روش‌شناسی سنجش ریسک سایبری.....
- ۱۱۴-۵-۱-۴-۱ مستند ۳۰-۸۰۰.....
- ۱۱۵-۵-۱-۵ نمونه ارزیابی ریسک سایبری ۳۰-۸۰۰.....
- ۱۱۹-۵-۱-۵-۱ توصیف ریسک NIST برای سازمان‌های دولتی.....
- ۱۱۹-۵-۱-۵-۲ رتبه‌بندی تهدید تقابلی NIST.....
- ۱۱۹-۵-۱-۶ دیگر روش‌شناسی‌های 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	<b>فصل ششم: ارزیابی‌های حالت فعلی و هدف</b>
۱۳۵	..... ۱-۶ مقدمه ارزیابی‌ها
۱۳۶	..... ۲-۶ ارزیابی‌های حالت فعلی
۱۳۷	..... ۱-۲-۶ رده‌های ارزیابی‌ها
۱۳۷	..... 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

۱۵۹	فصل هفتم: سنجش عملکرد.....
۱۶۰	۱-۷ ارزیابی راهبرد.....
۱۶۰	۲-۷ شاخص‌های کلیدی ریسک (KRI-ها).....
۱۶۰	۳-۷ شاخص‌های کلیدی عملکرد (KPI-ها).....
۱۶۲	۴-۷ گزارش‌دهی در مورد راهبردها.....
۱۶۳	۱-۴-۷ اقدامات نگاشت شده به زیررده‌های NIST CSF.....
۱۶۳	۲-۴-۷ اقدامات نگاشت نشده به NIST CSF.....
۱۶۴	۳-۴-۷ نگاشت اقدام به CSF هر هدف.....
۱۶۴	۴-۴-۷ گزارش‌های پیشرفت طرح راهبردی.....
۱۶۴	۵-۴-۷ مقایسه حالت فعلی با نهایی.....
۱۶۶	۶-۴-۷ آماده‌سازی گزارش عملکرد سالیانه.....
۱۶۸	۵-۷ تعیین اقدامات جدید برای سال بعد.....
۱۶۸	۶-۷ فعالیت‌های پایان سال.....
۱۶۸	۱-۶-۷ تعریف پارامترهای هرم راهبرد.....
۱۶۹	۲-۶-۷ تدوین برنامه زمانی.....
۱۷۰	۳-۶-۷ تأیید ترکیب اعضای گروه راهبری.....
۱۷۱	۴-۶-۷ گزارش عملکرد به مدیریت ارشد.....
۱۷۱	۵-۶-۷ مسئولیت‌های RACI کمیته راهبری.....
۱۷۲	۶-۶-۷ اطمینان از تبعیت از مقررات.....
۱۷۲	۷-۶-۷ کامل کردن حلقه حکمرانی.....
۱۷۲	۱-۷-۶-۷ دیاگرام سازمان حکمرانی.....
۱۷۳	۲-۷-۶-۷ RACI بدنه حکمرانی راهبردی.....
۱۷۳	۳-۷-۶-۷ مسیر تأیید حکمرانی.....
۱۷۴	۸-۶-۷ چرخه حیات راهبرد.....
۱۷۷	فصل هشتم: چک لیست‌ها و شابلون‌ها.....
۱۷۷	۱-۸ راهنمای آماده‌سازی راهبرد.....
۱۷۸	۲-۸ گام ۱: پیش‌برنامه‌ریزی.....
۱۷۸	۱-۲-۸ چک لیست پیش‌برنامه‌ریزی.....
۱۷۹	۲-۲-۸ هرم ساختار راهبرد.....
۱۷۹	۳-۲-۸ تحلیل ساختار سازمانی و فرهنگی.....
۱۷۹	۴-۲-۸ کامل کردن RACI برای گام ۱.....
۱۷۹	۵-۲-۸ اعتبارسنجی عوامل موفقیت اساسی.....
۱۷۹	۶-۲-۸ ارزیابی آمادگی سازمانی.....

- ۱۸۰ ..... ۳-۸ گام ۲: مدیریت پروژه راهبرد.....
- ۱۸۰ ..... ۱-۳-۸ منشور پروژه.....
- ۱۸۰ ..... ۲-۳-۸ کامل کردن RACI برای گام ۲.....
- ۱۸۰ ..... ۳-۳-۸ توسعه RACI کامل برای فعالیت‌های کمیته راهبری.....
- ۱۸۰ ..... ۴-۳-۸ تحلیل جریان داده برای گام ۲.....
- ۱۸۰ ..... ۵-۳-۸ تدوین فهرست مطالب گزارش نهایی اولیه.....
- ۱۸۰ ..... ۴-۸ گام‌های ۳ و ۴.....
- ۱۸۰ ..... ۱-۴-۸ RACI برای گام‌های ۳ و ۴.....
- ۱۸۱ ..... ۲-۴-۸ تحلیل جریان داده برای گام‌های ۳ و ۴.....
- ۱۸۱ ..... ۳-۴-۸ نداشت حادثه به کنترل‌ها.....
- ۱۸۱ ..... ۵-۸ گام ۵: ارزیابی‌های حالت فعلی و هدف.....
- ۱۸۱ ..... ۱-۵-۸ RACI برای گام ۵.....
- ۱۸۱ ..... ۲-۵-۸ تحلیل جریان داده برای گام ۵.....
- ۱۸۱ ..... ۳-۵-۸ انجام ارزیابی ریسک کمی.....
- ۱۸۱ ..... ۶-۸ گام ۶: سنجش عملکرد طرح و فعالیت‌های آخر سال.....
- ۱۸۱ ..... ۱-۶-۸ چک لیست برای گام ۶: فعالیت‌های آخر سال.....
- ۱۸۲ ..... ۲-۶-۸ RACI برای گام ۶.....
- ۱۸۲ ..... ۳-۶-۸ دیاگرام جریان داده برای گام ۶.....
- ۱۸۲ ..... ۴-۶-۸ استخراج عوامل اساسی موفقیت.....
- ۱۸۲ ..... ۵-۶-۸ بررسی شاخص‌های کلیدی ریسک و عملکرد.....
- ۱۸۲ ..... ۶-۶-۸ شابلون گزارش‌دهی طرح راهبردی.....
- ۱۸۲ ..... ۷-۶-۸ نداشت اقدام به CSF برای هر هدف.....
- ۱۸۲ ..... ۸-۶-۸ گزارش سالیانه امنیت و تاب‌آوری سالیانه.....
- ۱۸۲ ..... ۹-۶-۸ بستن حلقه حکمرانی.....
- ۱۸۳ ..... ۱۰-۶-۸ سلسله‌مراتب سازمان تأیید حکمرانی.....
- ۱۸۳ ..... ۱۱-۶-۸ RACI تأیید حکمرانی.....
- ۱۸۳ ..... ۱۲-۶-۸ مسیر حرکت تأیید حکمرانی.....
- ۱۸۳ ..... ۷-۸ سر هم کردن RACI پروژه کامل.....
- ۱۸۳ ..... ۸-۸ فایل‌های قابل دانلود کردن فصل ۸.....



