Gartner®

IT Roadmap for Cybersecurity

Excerpt

چگونه سازمان های موفق برنامه های امنیتی مبتنی بر ریسک را برای حمایت از چابکی و انعطاف پذیری کسب وکار توسعه می دهند؟

تحول کسب وکار دیجیتال و سیستم های فیزیکی-سایبری در حال ظهور، خطر امنیتی بی سابقه ای ایجاد می کند.

تا سال 2027، 75 درصد از کارمندان فناوری خارج از حوزه فناوری اطلاعات را به دست خواهند آورد، تغییر می دهند یا ایجاد می کنند.

در پاسخ، بسیاری از سازمان ها رویکردهای جدید امنیت سایبری را اتخاذ می کنند.

اما سازمان ها برای ایجاد تعادل بین امنیت سایبری و نیاز به اداره تجارت تلاش می کنند.

افسران ارشد امنیت اطلاعات می توانند با توسعه فرآیندهایی که امکان تصمیم گیری مبتنی بر ریسک را فراهم می کند و در عین حال از تهدیدات امنیتی محافظت می کنند و از نقض داده ها و سایر رویدادهای امنیت سایبری جلوگیری می کنند، کمک کنند.

از تحقیقات تخصصی و تعاملات خود با هزاران شرکت در سراسر صنایع، بهترین شیوه های امنیت سایبری را در یک نقشه راه قابل تنظیم گردآوری کرده ایم. از این نقشه راه برای درک مراحل کلیدی، منابع و افراد مورد نیاز برای برنامه ریزی و اجرای یک ابتکار امنیت سایبری موثر استفاده کنید.

67%

مدیران اجرایی و مدیران ارشد کسب وکار می خواهند کارهای فناوری بیشتر به طور مستقیم در بخش های تجاری و کمتر در فناوری اطلاعات انجام شود.

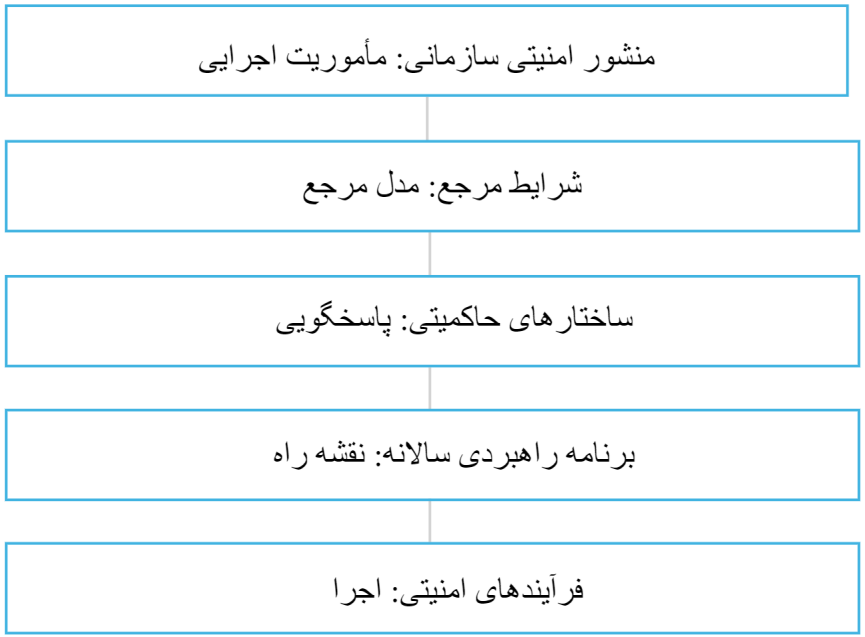
Source: 2022 Gartner CEO and Senior Business Executive Survey

با توسعه و اجرای یک برنامه امنیت سایبری قوی و قابل دفاع

تنها راه مقابله موثر با خطرات در حال تحول دیجیتالی شدن و افزایش تهدیدات سایبری، ایجاد یک برنامه امنیتی مستمر است. متأسفانه، بسیاری از سازمان ها زمانی که قصد ایجاد یک قابلیت امنیتی را دارند، فقط چک می زنند - یعنی معمولاً اسناد زیادی تولید می کنند و به شدت در فناوری سرمایه گذاری می کنند.
اما آنها زمان کمی را صرف ایجاد حکمرانی مؤثر یا توانایی ارزیابی و تفسیر مؤثر ریسک می کنند.

یک برنامه امنیتی قابل دفاع پاسخ به سوال مهم ذینفعان را اثبات می کند:
آیا سازمان به اندازه کافی برای محافظت معقول از منابع اطلاعاتی خود انجام می دهد؟

اجزای یک برنامه امنیت سایبری



Source: Gartner

برخی از سوالات اصلی طرح امنیت سایبری عبارتند از:

1 چگونه از انعطاف پذیری و اهداف رشد کسب و کار حمایت می کند و در عین حال ریسک را کاهش می دهد؟

2 چگونه می توانیم از رویکرد نتیجه محور برای تعیین اولویت ها و سرمایه گذاری های امنیت سایبری استفاده کنیم؟

3 کدام رهبران و تیم ها باید درگیر شوند؟

مراحل کلیدی چیست؟

این بینش بهترین عملکرد از تعامل با مشتریانی که ابتکارات امنیت سایبری را با موفقیت اجرا کرده اند، استخراج می شود.
این نقشه توالی اهداف و نتایج مورد نظر را نشان می دهد و برای همسویی همه ذینفعان مفید است.

چند نقطه عطف کلیدی و نمونه ای از منابع گارتنر مرتبط در زیر برجسته شده است،
اما نقشه راه کامل شامل جزئیات کامل تمام نقاط عطف و منابع برای هر مرحله خواهد بود.

ارزیابی مجدد و بهینه سازی | ساختن و برنامه بالغ | اجرا را آغاز کنید | برنامه اقدام را توسعه دهید | تراز کردن استراتژی

برنامه اقدام را توسعه دهید

چارچوب اولویت بندی ریسک را ایجاد کنید

وظایف انتخاب شده

- انجام ارزیابی آسیب پذیری و تست نفوذ
- خط پایه سررسید فعلی را تعیین کنید، وضعیت هدف را تعریف کنید و تجزیه و تحلیل شکاف را انجام دهید
- خرید و پشتیبانی از منابع اجرایی یا هیئت مدیره دریافت کنید
- معماری امنیتی، چارچوب سیاست و لایه راه حل را توسعه دهید

نمونه منابع مرتبط گارتنر

- **Research:** CISO Foundations — Toolkit: Strategic Planning Presentation and Dashboards
- **Tool:** IT Score for Security and Risk Management
- **Research:** Ignition Guide to Building an Annual Cybersecurity Budget

+ more

تراز کردن استراتژی

اهداف را تعیین کنید و مورد تجاری بسازید

وظایف انتخاب شده

- درک اولویت های کلیدی کسب و کار؛ تعریف ماموریت و چشم انداز برنامه؛ و محرک های تجاری، فناوری و تهدید را شناسایی کنید.
- اهداف، ارزش برنامه و نقش ها و مسئولیت های ذینفعان کلیدی را شناسایی کنید.
- کنترل های امنیتی را در راستای استراتژی های سازمانی تعریف کنید و آنها را به یک چارچوب امنیتی استاندارد ترسیم کنید
- دریافت بازخورد سهامداران، تعریف اهداف کلیدی و نهایی کردن خلاصه اولیه سند استراتژی امنیتی

نمونه منابع مرتبط گارتنر

- **Analyst inquiry:** Engage with an analyst to finalize the right metrics that can measure the impact of cybersecurity
- **Analyst inquiry:** Engage with an analyst to discuss the right approach to communicate the business impact of cybersecurity to the stakeholders
- **Research:** How to Build a Robust, Defensible Security Program That Enables Business Growth and Agility

+ more

برنامه بسازید و بالغ کنید

از طریق حاکمیت، مسئولیت پذیری و اطمینان را حفظ کنید

وظایف انتخاب شده

- ☐ توسعه قابلیت پاسخ به حوادث بحرانی و یک برنامه اقدام در صورت بروز تخلف
- ☐ یک ساختار برنامه برای نظارت و مبارزه با تهدیدات پیشرفته ایجاد کنید
- ☐ فرهنگ رفتار امن کارکنان را القا کنید و کمپین های آموزشی و آگاهی را آغاز کنید
- ☐ ایجاد گزارش و پاسخ پیشرفته و ایجاد یک برنامه ارتباطی برای نقض سایبری

نمونه منابع مرتبط گارتنر

- **Analyst inquiry:** Engage with an analyst to finalize the right metrics that can measure the impact of cybersecurity
- **Analyst inquiry:** Engage with an analyst to discuss the right approach to communicate the business impact of cybersecurity to the stakeholders
- **Research:** How to Build a Robust, Defensible Security Program That Enables Business Growth and Agility

اجرا را آغاز کنید

طراحی و تنظیم ساختار تیم

وظایف انتخاب شده

- ☐ قابلیت ها، ابزارها و فناوری ها را یکپارچه کنید
- ☐ نقش ها و مسئولیت های تیم امنیتی را تعیین کنید و ذینفعان را شناسایی کنید تا پاسخگو، مشورت و مطلع باشند.
- ☐ شایستگی های حیاتی را توسعه دهید و برای مهارت های مورد نظر از دست رفته آموزش دهید
- ☐ از معیارها و مشوق ها برای ایجاد مسئولیت در بین مالکان استفاده کنید

نمونه منابع مرتبط گارتنر

- **Consultation by phone:** Engage with an expert to discuss “The CARE Standard for Cybersecurity”
- **Research:** Read about cybersecurity threat and its impact on the business
- **Research:** How to Design a Practical Security Organization

ارزیابی مجدد و بهینه سازی

ارتباط با ارزش برنامه

وظایف انتخاب شده

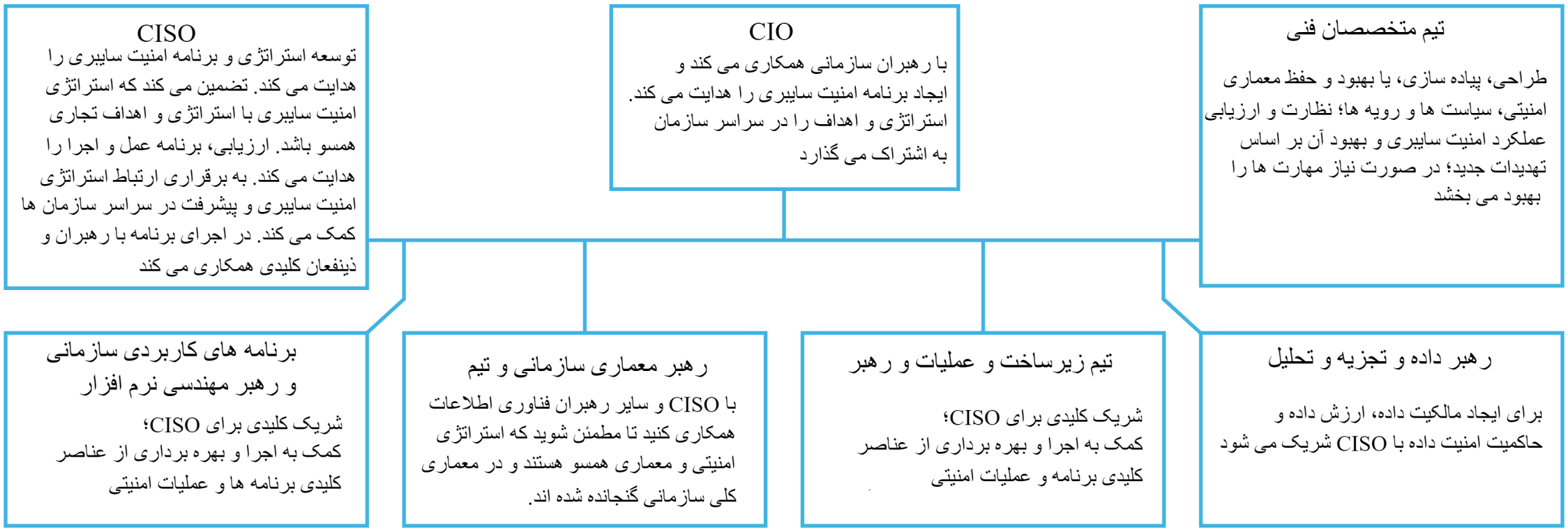
- [ ] برنامه ای برای انتقال ارزش به سازمان و هیئت مدیره ایجاد کنید
- [ ] معیارها را دنبال کنید و برای ارزیابی و بهبود اثربخشی برنامه به دنبال بازخورد باشید
- [ ] برای بهینه سازی بیشتر، ارزیابی بلوغ را دوباره بررسی کنید

نمونه منابع مرتبط گارتنر

- **Consultation by phone:** Discuss the key points that can help in the further optimization of cybersecurity preparation in the organization
- **Analyst inquiry:** Redo the Gartner IT Score assessment to measure progress and reprioritize
- **Research:** Tool — Board Briefing: How to Communicate the Cyber-Risk Posture of Your Organization

چه کسی باید درگیر شود؟

موفق ترین شرکت ها برای ابتکارات امنیت سایبری خود تیم های متقابل ایجاد می کنند.
ما کارکردهای توصیه شده برای مشارکت و نقش آنها را برای اطمینان از بهترین موفقیت در رسیدن به نقاط عطف بیان کرده ایم.



داستان موفقیت مشتری:
فعال کردن انطباق فناوری اطلاعات با نقشه راه امنیت سایبری

با کمک گارتنر توانست:

- رویکردی جامع به رویه های حاکمیتی و مدیریت ریسک داشته باشد.
- پایه و اساس کسب و کار دیجیتالی قوی بسازد
- فرآیندهای تجاری را بهینه کند، در زمان و انرژی برای مدیریت ارشد صرفه جویی کند.

Pacific Textiles با دسترسی به کارشناسان، تحقیقات و ابزارهای گارتنر توانست اطلاعات را از طریق یک سیستم ERP دیجیتالی کند،
فرآیندهای تولید را با فناوری جدید خودکار کند و یک نقشه راه امنیتی سایبری آماده برای اجرا ایجاد کند.

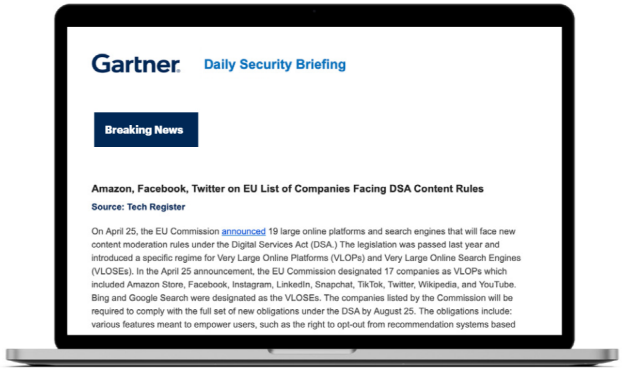
Pacific Textilesبا هدف ساده سازی فرآیندهای کسب وکار و ایجاد یک محیط آماده برای تجارت دیجیتال، می خواست چارچوبی را ایجاد کند که به انطباق با فناوری اطلاعات پایبند باشد و خطر امنیت سایبری را به حداقل برساند.

گارتنر برای افسران ارشد امنیت اطلاعات

با راهنمایی های متخصص، ابزارها، شبکه های همتا و رویدادهای هدفمند، ارزش را در سراسر تجارت افزایش دهید.

گزارش امنیتی روزانه

Stay on top of the most pressing news with a digest of articles from reputable news sources, including a cross-industry, global summary of the most recent threats and security news of the day.



»این اولین چیزی است که هر روز صبح می خوانم. من از آن برای رفع نگرانی هایی که از سوی مدیران اجرایی می آیند و هرگونه آسیب پذیری جدید را برای تیمم ارسال می کنم استفاده می کنم تا اطمینان حاصل کنم که اقداماتی را برای کاهش ریسک انجام می دهیم.«

ارائه دهنده جهانی فناوری بی سیم ciso

تسریع ابتکارات کلیدی

با ابزارهایی که اجرا را تسریع می کنند و نتایج کسب وکار را به ارمغان می آورند، استراتژی را به عمل تبدیل کنید:

- تشخیص اثربخشی OSIC
- ارزیابی کنترل های امنیت سایبری
- امتیاز فناوری اطلاعات
- قالب های توجیهی هیئت مدیره

شبکه های همتا

با سایر رهبران صنعت امنیت در چت های 1:1، بحث های همتا، نظرسنجی ها، و دسترسی به رتبه بندی ها و بررسی های فناوری ارتباط برقرار کنید.

رویدادهای جذاب

از دسترسی VIP در اجلاس امنیت و مدیریت ریسک گارتنر با جلسات متعدد آموزشی و فرصت های بسیار بیشتر برای ارتباط با همتایان و کارشناسان گارتنر لذت ببرید. به علاوه، برای حضور در حلقه CISO برای جلسات انحصاری و فرصت های شبکه درخواست دهید.

نشان دادن ارزش تجاری

رهبر امنیت سایبری بهتری در زمینه های کلیدی باشید:

- نقش، روابط، استعداد و فرهنگ
- اخذ بودجه های قابل دفاع
- استراتژی و چشم انداز برنامه امنیت سایبری

با برنامه های قوی امنیت سایبری روزانه از خطر اجتناب کنید:

- مدیریت ریسک شرکت
- آینده کار، استراتژی های واکنش به ریسک، مدیریت تغییر

بهینه سازی سرمایه گذاری و اجرای فناوری:

- روند پیشرفت های فناوری نوظهور
- ابزارهای اندازه گیری و تصمیم گیری عملی
- راهنمای پیاده سازی فنی عمیق
- بینش صنعت متنی

بینش عملی و عینی

این منابع و ابزارهای اضافی را برای رهبران امنیت سایبری جستجو کنید:

Research

The CISO's Guide to Your First 100 Days

Find out the actions you should take in your first 100 days as a CISO.

Webinar

Treat Cybersecurity as a Business Investment for Better Outcomes

Understand how to communicate outcome-driven metrics to your board of directors.

eBook

Leadership Vision for Security and Risk Management Leaders

Explore the top 3 strategic priorities for security and risk management leaders.

Conference

Explore Gartner Cybersecurity Conferences

Advance your cybersecurity and risk management strategy by attending a Gartner conference.

Access other roadmaps in this series

Protect Your Business Assets With a Roadmap for Maturing Information Security

Roadmap: Drive Successful Digital Growth With Data and Analytics

Migrating Data and Analytics Architectures to the Cloud: Roadmap

Enhance Your Roadmap for Effective Data Governance

Roadmap: Devising an Effective Cloud Strategy

با ما در تماس باشید

شرکت "داده پردازی هوشمند کندو" درسال 1402 به منظور ارائه خدمات فناوری اطلاعات و ارتباطات به ویژه در حوزه امنیت اطلاعات تاسیس گردید.
هدف اصلی ما ارائه راهکارهای جامع امنیت، جهت حفاظت از اطلاعات و دارایی های دیجیتال سازمان ها می باشد. در تلاش هستیم با خدمات مشاوره، اجرا، پیاده سازی و راهبری پروژه ها و همچنین ارائه راهکارهای نوآورانه و انعطاف پذیر، به نیازها و انتظارات بازار پاسخ دهیم.
ما با توسعه دانش و مهارت کارکنان خود، به افزایش بهره وری و ارزش آفرینی می پردازیم.

www.csdpc.ir
info@csdpc.ir