Gartner for IT Leaders

The CISO's Guide to Your First 100 Days

By William Candrick, Sam Olyaei, Tom Scholtz

Gartner

The CISO's Guide to Your First 100 Days

Published 24 May 2021 - ID G00747118 - 20 min read

By Analyst(s): William Candrick, Sam Olyaei, Tom Scholtz

Initiatives: Security and Risk Management Leaders

صد روز اول شما در نقش افسر ارشد امنیت اطلاعات (یا معادل) آن موفقیت شما را به عنوان یک رهبر مدیریت امنیت و ریسک تعیین می‌کند. گارتنر راهنمایی و پشتیبانی برای کمک به CISO های جدید برای به حداکثر رساندن موفقیت خود را در این مرحله انتقال فراهم می‌کند.

بررسی اجمالی

یافته های کلیدی

■ مدیران ارشد امنیت اطلاعات CISO در درجه اول رهبران، مدیران و ارتباطات هستند – نه فناوران

■ موفقیت یک CISO به دو دستاورد مهم بستگی دارد:
ایجاد یک برند شخصی از اعتبار و رهبری
پایه گذاری یک برنامه امنیتی قابل دفاع

■ CISOهای جدید زمانی که در درک انتظارات رهبری شکست می خورند یا نمی توانند به طور موثر ارتباط برقرار کنند که چگونه امنیت از نتایج کسب و کار حمایت می کند با مشکل مواجه می شوند.

توصیه‌ها

برای رهبران امنیتی و مدیریت ریسک در صد روز اول خود در نقش CISO

■ با پیوند دادن اولویت های رهبری خود به نتایج و اهداف تجاری، رابطه برنامه امنیت سایبری با تجارت را تقویت کنید.
■ قبل از فرو رفتن در جزئیات فنی و تصمیمات فناوری، یک استراتژی برای امنیت تعریف کنید.
■ با شناسایی دو تا پنج اولویتی که می توانید در صد روز اول انجام دهید، شانس موفقیت خود را به حداکثر برسانید.
■ برای جلوگیری از به تاخیر انداختن ابتکارات استراتژیک، زمان اضافی را برای حوادث امنیتی غیرقابل پیش‌بینی قبل از وقوع اجتناب‌ناپذیر اختصاص دهید

■ با به اشتراک گذاشتن یک چشم انداز استراتژیک، نشان دادن چگونگی تناسب کارکنان با آن دیدگاه و اجتناب از انتقاد عمومی از پیشینیان، حمایت تیم امنیتی را به دست آورید

مقدمه

صد روز اول شما در نقش CISO فرصتی برای تعریف نقش و روابط حرفه‌ای خود است. این دوره کوتاه "ماه عسل" معمولا فرصتی را برای توسعه استراتژی، ایجاد ارتباطات، پشتیبانی رهبری ایمن، ایجاد اعتماد با تیم جدید و نشان دادن سبک رهبری شما فراهم می‌کند.
این فرصت به ویژه در صورتی ارزشمند است که شرکت به یک بازنگری اساسی در حاکمیت ریسک سایبری یا بوغ برنامه امنیتی به میزان قابل توجهی نیاز داشته باشد.

این تحقیق به بررسی این موضوع می‌پردازد که چگونه CISOهای پیشرو از صد روز اول خود استفاده کامل میکنند. ما این دوره را به شش مرحله تقسیم می‌کنیم: آماده‌سازی، ارزیابی، برنامه‌ریزی، اقدام، اندازه‌گیری و برقراری ارتباط

Figure 1: The CISO's First 100 Days Roadmap

Phases and Goals of a CISO's First 100 Days: Click links to jump to sections

هدف	فاز
برای نقش خود قبل از روز اول برنامه ریزی کنید	آماده کردن
بلوغ فعلی اوراق بهادار را درک کنید	ارزیابی کنید
یک نقشه راه برای صد روز اول ایجاد کنید	طرح
بهبودهای بلوغ قابل مشاده را اعمال کنید	عمل کنید
شواهدی از پیشرفت امنیت ارائه دهید	اندازه گرفتن

برنامه صد روز اول

به طور خلاصه، یک دستورکار موفق برای صد روز اول باید:

- اعتبار خود را به عنوان یک CISO ایجاد کنید و برند و تصویر داخلی شرکت امنیتی را ارتقا دهید.
- بلوغ فعلی برنامه امنیتی را تعیین کنید. به امتیاز IT برای امنیت و مدیریت ریسک مراجعه کنید.
- تمرکز بر زیر مجموعه ای از ابتکارات استراتژیک که با روش شناسایی قابل دفاع انتخاب و اولویت‌بندی می‌شوند. مانند: ارزیابی بلوغ، ارزیابی ریسک
- شکاف بین برتری عملیاتی امنیتی و ارزش تجاری
- اهداف واقعی، قابل اندازه گیری و محدود به زمان را تعریف کنید و معیارهایی برای پیگیری ایجاد کنید.

باقیمانده این یادداشت تحقیقاتی راهنمایی عملی برای دستیابی به این اهداف ارائه میدهد.

مرحله آماده‌سازی (قبل از روز اول)

قبل از اولین روز کاری خود را برای نقش جدید خود آماده کنید.
یک برنامه‌ریزی اولیه، زمینه را برای شروع موفقیت‌آمیز فراهم می‌کند و روابطی را که در طول مدت تصدی خود به عنوان یک CISO به آن نیاز دارید، ایجاد کند.

نتایج را برای مرحله آماده‌سازی، هدف قرار دهید:
هنگام آماده شدن برای نقش CISO، نتایج زیر را هدف قرار دهید:

- درکی مشترک از نقش خود و انتظارات کارکنان، سهلمداران ارشد و تیم رهبری
- یک برنامه مشارکت اساسی برای ملاقات با ذینفعان رهبری و کارکنان امنیتی

این مرحله بر گوش دادن و یادگیری متمرکز است – نه تصمیم‌گیری. از ساختن خودداری کنید.
اعلامیه‌ها یا تصمیمات گسترده در چند هفته اول شما در نقش CISO

اقدامات برای مرحله آماده سازی
اقدامات زیر را قبل از روع اولین روز خود انجام دهید:

نوع CISO مورد نیاز شرکت شما را ارزیابی کنید: بنگاه‌ها بر اساس فرهنگ، صنعت، چالش های سیاسی و عوامل دیگر نیازمندی های متفاوتی دارند. برخی به یک CISO مبتنی بر عملیات نیاز دارند، در حالی که برخی دیگر به یک CISO متمرکز بر تجارت نیاز دارند. گارتنر توصیه می‌کند که رهبران مدیریت ریسک و امنیت، شاخص اثربخشی CISO را مشاهده کنند و بر اساس نیازهای شرکت خود روی توسعه پروفایل‌ها کار کنند.

ساختار شرکت خود را درک کنید: برای درک ساختار امنیت، فناوری اطلاعات و کل سازمان، نمودارهای سازمانی و اسناد عملیاتی به عنوان مثال، نقشه های فرایند را درخواست کنید. اطمینان حاصل کنید که حاکمیت فعلی و نقش عملیاتی امنیت در شرکت را درک کرده اید.

ذینفعان کلیدی را شناسایی کنید: فهرستی از ذینفعان رهبری که با آنها کار خواهید کرد ایجاد کنید. این فهرست ممکن است شامل مشاور عمومی، رئیس منابع انسان، افسر ارشد حریم خصوصی و افسر ارشد ریسک باشد، اما محدود به آن نیست.

ارتباطات جدید ایجاد کنید: با ذینفعان رهبری و کارکنان امنیتی، به طور ایده آل قبل از اولین روز در نقش خود، درگیر شوید. تاکتیک های نامزدی شامل یادداشت های تشکر پس از مصاحبه و ارتباط لینکداین (با یادداشت های شخصی سازی شده است.)

جلسات اولیه را برنامه ریزی کنید: با دستیار اداری خود یا یک مخاطب دوستانه در شرکت کار کنید تا دور اولیه جلسات خود را تنظیم کنید. یک جلسه تیم امنیتی همه جانبه در روز اول و یک سری ملاقات و حوشامدگویی در هفته اول با سهامداران کلیدی در سراسر سازمان برنامه ریزی کنید.
چند هفته اول فرصتی برای معرفی و تثبیت خود در سازمان است.

ارتباطات در مرحله آماده سازی
ارتباطات در مرحله آماده سازی قبل از روز اول، تمرکز شما در درجه اول باید بر روی یادگیر در مورد شرکت و تهیه پیام برای سهامداران و تیم شما باشد. موفقیت در چند هفته ابتدایی شما به ارتباط موثر بستگی دارد – نه تصمیم‌گیری

قبل از روز اول و در هفته ها اولیه حضور در نقش، روی موارد زیر تمرکز کنید:

اولویت های C-suite's خود را درک کنید: دستیابی به پتانسیل کامل خود به عنوان یک CISO مستلزم درک کسب و کار شرکت شما و اولویت هایی است که برای C-suite's و هئیت مدیره در نظر گرفته می‌شود. منابع اطلاعاتی زیر را قبل از اولین روز خود در نظر بگیرید:

■ بیانیه ماموریت شرکت خود را از صفحه وب درباره ما بیاموزید.

■ اولویت ها و نگرانی های رهبری را با مطالعه پرونده‌های مالی اخیر عمومی درک کنید
پرونده ها به عنوان مثال، گزارش های 10-Q یا 10-K برای شرکت های تجاری ایالات متحده

■ ارتباطات و مصاحبه های اخیر رهبری را بخوانید و تماشا کنید و حساب‌های رسانه های اجتماعی رهبری را دنبال کنید

■ هرگونه اولویت‌های رقیب را در C-suite شناسایی کنید و برای عبور از امنیت از طریق این پیچیدگی های رهبری آماده شوید.

خودتان را معرفی کنید: یک بیوگرافی کوتاه ایجاد کنید که پیشینه شخصی، مسیر شغلی و افکار اولیه شما در مورد پیوستن به شرکت را پوشش دهد. از این Bio در ارائه ها و ملاقات و احوال‌پرسی استفاده کنید تا همه بفهمند شما کی هستید و از کجا آمده اید.
در این مقدمه های اولیه از اعلام تصمیمات جسورانه و مخرب خودداری کنید. بلکه هدف اصلی شما این است که مورد استقبال همسالان و تیم خود قرار بگیرید.

از داستان سرایی استفاده کنید: قصه گویی راهی موثر برای تغییر دیدگاه ها و جلب پذیرش است. به عنوان مثال، یک CISO جدید ممکن است داستانی را بیان کند که نشان می‌دهد چگونه نقش امنیت در کمک به شرکت در حرکت سریع و ایمن است - نه کاهش سرعت کارها به منظور کاهش هر خطر تا حد ممکن. ارائه یک مثال گویا از تجربه یا رویدادهای گذشته در اخبار به ذینفعان کمک می کند تا بفهمند که چگونه امنیت، و در نتیجه CISO، یک منبع است - نه یک مانع.

راهنمای بحث ایجاد کنید: قبل از دور اولیه جلسات ملاقات و احوال‌پرسی، سؤالات و نکات گفتگو را آماده کنید. برای مثال موارد زیر را در نظر بگیرید:

■ **بحث‌های ذینفعان:** برای این جلسات، بر درک سهامداران از امنیت و نقش CISO تمرکز کنید. جمع آوری این اطلاعات در اوایل صد روز اول به شما کمک می کند تا تغییرات را در ماه های آینده برنامه ریزی کنید، از جمله تغییر دیدگاه های رهبری و (دوباره) تعریف نقش CISO سوالاتی که باید بپرسید عبارتند از

■ فوری ترین اولویت های کاری شما چیست؟
■ برداشت فعلی شما از عملکرد امنیتی چیست؟
■ بزرگترین نقاط درد شما هنگام کار با امنیت چیست؟
■ کار با امنیت به خوبی پیش می‌رود؟

■ **بحث‌های کارکنان:** سوالاتی را آماده کنید که (1) وضعیت فعلی حاکمیت و عملیات امنیتی و (2) درک کارکنان از تیم و محیط کار را تشخیص دهد.
سوالاتی که باید بپرسید عبارتند از

■ بیشتر وقت خود را کجا متمرکز می کنید؟
■ چه چیزی کار شما را آسان می کند؟
■ چالش برانگیزترین نقش شما چیست؟
■ چگونه می توانم بهتر از شما و تیمتان حمایت کنم؟
■ به نظر شما اولویت های امنیتی باید چه باشد؟
■ اهداف اصلی شرکت را چه می‌بینید؟

منابع برای مرحله آماده سازی

برای شروع، منابع گارتنر زیر را مرور کنید.

تحقیق و ابزار گارتنر

نقشه راه برای اثربخشیCISO - رویکرد رهبری خود را براساس بهترین شیوه های اثبات شده که از CISO های پیشرو تهیه شده است، تنظیم کنید.

توسعه مهارت های CISO معاصر - شناسایی و ایجاد مهارت ها برای توسعه به یک CISOجامع و توانا.

اثربخشیCISO: گزارشی در مورد رفتارها و طرز فکرهایی که بر اثربخشی CISO تأثیر می گذارد - رفتارها و طرز فکرهایی را که بیشترین ارتباط را با اثربخشی CISOدارند، شناسایی کنید.

مرحله ارزیابی هفته اول تا چهارم

بلوغ و عملکرد فعلی اوراق بهادار را ارزیابی کنید. ارزیابی امنیت با کیفیت شکاف هایی را نشان می‌دهد که برنامه ریزی استراتژیک را مشخص می کند. CISOهای موفق به جای غریزه، بر ارزیابی‌های عینی تکیه می کنند تا تصمیم گیری قابل دفاع و تکرار باشد.

نتایج هدف برای مرحله ارزیابی

هنگام ارزیابی برنامه امنیتی، نتایج زیر را هدف قرار دهید:

■ یک مربی اجرایی که بینشی را در مورد فرهنگ شرکت ارائه می دهد. درک درستی از منابع در دسترس شما از جمله بودجه، تعداد کار و فناوری.

■ فهرستی از شکاف های امنیتی از طریق ارزیابی های رسمی بلوغ، گفتگوهای تیمی و مشارکت ذینفعان ظاهر شد.

■ فهرست اولویت بندی شده از سه تا پنج اولویت استراتژیک که به شکاف های امنیتی می پردازد و با نتایج کسب و کار همسو می شود.

اقدامات برای مرحله ارزیابی

اقدامات زیر را در اولین ماه نقش خود انجام دهید:

به دنبال یک مربی اجرایی باشید: یکی از با ارزش ترین دارایی های شما یک مربی در سطح ارشد خواهد بود. به دنبال رهبری باشید که بینشی نسبت به عملکرد درونی کارکنان ارشد اجرایی داشته باشد. دانش در زمینه امنیت ضروری نیست. در واقع، اگر مربی شما اطلاعات کمی در مورد امنیت داشته باشد، به بهترین وجه به شما خدمت خواهد کرد تا درک واقعی و عینی از نحوه دریافت پیشنهادات و رهبری خود به دست آورید.

نقش‌ها و مسئولیت‌های امنیتی را تعیین کنید: اولین اولویت شما در نقش CISO شفاف‌سازی و تعریف نقش‌ها و مسئولیت‌های امنیتی است. با مدیر خود بحث کنید تا عملکرد امنیتی و نقش خود را به طور کامل بررسی کنید. شفاف سازی مالکیت در زمینه هایی مانند:

- امنیت فیزیکی
- تداوم کسب و کار و بازیابی فاجعه BC/DR
- حریم خصوصی
- رعایت
- ریسک فناوری اطلاعات
- حاکمیت ریسک
- عملیات امنیتی

برای مناطق خارج از صلاحیت امنیتی، اطمینان حاصل کنید که با مدیران و رهبران همتا (مانند رئیس ERM، افسر ارشد حریم خصوصی، مشاور عمومی) روابط کاری ایجاد می‌کنید.

منابع اطلاعاتی خود را تهیه کنید: به سرعت فهرستی از منابع اطلاعاتی را که برای مدیریت عملکرد امنیتی به آن نیاز دارید، تهیه کنید. به عنوان مثال، هرگونه خط مشی موجود، نمودار سازمانی، برنامه های استراتژیک، پروژه های جاری، نقشه راه فناوری و معیارها را پیدا کنید. از این منابع اطلاعاتی برای آگاه کردن درک خود از وضعیت فعلی و برنامه های فوری امنیتی استفاده کنید

انجام ارزیابی های بلوغ: یک محیط امن برای کارکنان امنیتی ایجاد کنید تا به طور صریح بلوغ امنیت را ارزیابی کنند. این ارزیابی‌ها شکاف‌هایی را نشان می‌دهند که از تنظیم استراتژی آینده‌نگر خبر می‌دهند - نه سرزنش عقب‌نگر. به عنوان یک CISO جدید، حداقل باید ارزیابی‌های اصلی زیر را انجام دهید و در صورت امکان، موارد دیگری را اضافه کنید.

ارزیابی های اصلی برای صد روز اول:

■ **ارزیابی بلوغ عملکردی:** ارزیابی قابلیت امنیت و بلوغ فرآیند. امتیاز فناوری اطلاعات گارتنر را برای مدیریت امنیت و ریسک در نظر بگیرید.

■ **ارزیابی بلوغ کنترل:** بلوغ اجرای کنترل های امنیتی را ارزیابی کنید. سرویس سنجش بلوغ کنترل‌های گارتنر را در نظر بگیرید.

■ **ارزیابی ریسک:** ریسک های اطلاعاتی مرتبط با برنامه ها و زیرساخت ها را در سراسر سازمان ارزیابی کنید. ارزیابی‌های ریسک باید برای بالاترین حوزه های ریسک اولویت بندی شوند و اطلاعات جمع آوری شده در هر ثبت ریسک موجود ممکن است به ارزیابی وضعیت ریسک شرکت شما کمک کند.

ارزیابی های اضافی:
■ یافته های حسابرسی
■ ارزیابی آسیب پذیری
■ ارزیابی تهدید
■ سنجش استعداد
■ یافته های نظارتی
■ تست های نفوذ
■ تست های فیشینگ

اولویت های استراتژیک خود را شناسایی کنید: انجام ارزیابی ها شکاف هایی را که در سراسر برنامه امنیتی وجود دارد آشکار می کند. از این شکاف ها برای شناسایی سه تا پنج اولویت استراتژیک که باید در صدر روز اول خود به آن توجه کنید، استفاده کنید. این اولویت ها باید به چالش های اساسی بپردازند و تأثیر مثبتی بر تیم امنیتی و رهبری ارشد بگذارند.

اولویت هایی را در نظر بگیرید که:
■ به الزامات اساسی برای یک برنامه امنیتی موفق رسیدگی کنید
■ به وضوح به نتایج کسب و کار پیوند دهید
■ پایه ای برای بهبود سررسید چند ساله فراهم کنید
■ اعتبار خود را به عنوان یک CISO و افسر موثر شرکت ایجاد کنید

ارتباطات در مرحله ارزیابی
ارزیابی وضعیت فعلی امنیت می تواند یک فرآیند چالش برانگیز باشد. برای مثال، برخی از کارکنان امنیتی ممکن است شکاف‌ها را به حداقل برسانند، زیرا احساس دفاعی می‌کنند یا ترجیح می‌دهند چیزها را به بهترین شکل ممکن ارائه دهند. برعکس، سایر کارکنان امنیتی ممکن است برای کسب سرمایه گذاری و حمایت برای اولویت های محدود خود، شکاف ها را اغراق کنن. به یاد داشته باشید، اینها تمایلات طبیعی انسان هستند و می توان با ایجاد یک محیط باز، ایمن و شفاف با آنها مقابله کرد.

بر فرصت های ارتباطی زیر تمرکز کنید:

■ **ملاقات با رهبران تیم:** جلسات انفرادی با رهبران تیم امنیتی برگزار کنید. نظرات آنها را در مورد وضعیت فعلی برنامه امنیتی بسنجید و روشن کنید که هر یک از رهبران نقش اساسی در تعیین استراتژی امنیتی اجرایی در هفته ها، ماه ها و سال های آینده ایفا می کند.

■ **مصاحبه با سهامداران:** با سهامداران مصاحبه کنید و برداشت های آنها را از عملکرد امنیتی جمع آوری کنید. ذینفعان مورد هدف شامل مشاور عمومی، افسر ارشد حفظ حریم خصوصی، CIO، مدیر اجرایی حسابرسی و رئیس HR هستند.

■ **اینفلوئنسرها را شناسایی کنید:** همانطور که با رهبران شرکت ملاقات می کنید، اینفلوئنسرهای ارشد را یادداشت کنید که می توانند اولویت های امنیتی را پیش ببرند، به شما یک دستور شخصی بدهند و به شما کمک کنند تا برای ارتباطات در سطح ارشد و هیئت مدیره آماده شوید.

منابع برای مرحله ارزیابی
برای شروع، منابع گارتنر زیر را مرور کنید.

تحقیق و ابزار گارتنر
امتیاز فناوری اطلاعات برای مدیریت امنیت و ریسک - بلوغ فرآیندها و قابلیت‌های عملکرد امنیتی خود را ارزیابی کنید.

خدمات سنجش بلوغ کنترل - بلوغ کنترل‌های فنی خود را با همتایان مشابه خود محک بزنید.

مرحله طرح (هفته سوم الی ششم)

مرحله طرح، اطلاعات حاصل از ارزیابی های شما را در طرحی برای اقدام ترکیب می کند. برنامه‌ریزی اولیه شما نقشه راه صد روز اول شما را تعیین می کند و موفقیت امنیت را در اولین سال حضور شما در این نقش هدایت می کند.

نتایج هدف برای مرحله طرح
درحین انجام برنامه ریزی، نتایج زیر را هدف قرار دهید:

■ یک **برنامه استراتژیک مستند** که دو تا سه ابتکار امنیتی را برای صد روز اول شما اولویت بندی می کند و یک نقشه راه است برای سال اول شما.

■ یک **بودجه عملیاتی** که منابع کافی برای دستیابی به اولویت ها را تضمین می کند. درصورت کمبود منابع، برنامه استراتژیک باید براساس آن تنظیم شود تا قابل دستیابی باشد.

اقدامات برای مرحله طرح
هنگام انجام برنامه ریزی اقدامات زیر را انجام دهید:

چند اولویت اصلی را انتخاب کنید: اولویت های اصلی خود را بررسی کنید و دو تا سه اولویت را انتخاب کنید تا درسه ماه آینده روی آنها تمرکز کنید. ازمعیارهای زیر برای فیلترکردن این اولویت‌ها استفاده کنید:

■ آیا می توان درعرض سه ماه به ابتکار عمل دست یافت؟
■ آیا حمایت اجرایی، منابع و بودجه مورد نیاز را خواهید داشت؟
■ آیا این ابتکار با کاهش خطرات سایبری مرتبط است؟
■ آیا خطر شکست نسبتاً کم است؟

همانطورکه اولویت ها را انتخاب می کنید، به رهبران کسب و کار کمک کنید تا بفهمند اولویت های امنیتی چگونه ازنتایج کسب و کار پشتیبانی می کنند. برقراری زودهنگام این اتصال اعتباری را که شما و عملکرد امنیتی برای دستیابی به اولویت های استراتژیک دریافت می کنید، به حداکثر می رساند.

عملکرد امنیتی خود را طراحی یا اصلاح کنید: عملکرد امنیتی را براساس وظایف، اولویت ها و فرهنگ سازمانی خود ساختار دهید. متأسفانه، هیچ رویکرد یکسانی برای طراحی سازمان امنیتی وجود ندارد. بلکه باید عملکرد را به گونه ای طراحی کنید که نقش ها و مسئولیت ها روشن باشند، مدیران توانمند و پاسخگو باشند، و ارتباطات با همتایان خارج ازامنیت (به عنوان مثال، فناوری اطلاعات، حریم خصوصی) روشن است.

بودجه عملیاتی خود را برنامه ریزی کنید: سطح کنترل شما بربودجه امنیتی به زمان پیوستن شما به شرکت (ابتدا، اواسط یا پایان سال مالی) و فرآیند بودجه ریزی فعلی بستگی دارد. درحالی که برخی ازجنبه‌های بودجه بندی ممکن است درطول صد روزاول شما انعطاف‌پذیر نباشد، باید اطمینان حاصل کنید که بودجه عملیاتی شما می تواند ازاولویت های استراتژیک شما پشتیبانی کند. ممکن است تخصیص مجدد منابع برای حمایت از اولویت ها را درنظر بگیرید.

ارتباطات در مرحله طرح

یک برنامه استراتژیک امنیتی را مستند کنید: برنامه استراتژیک صد روزه اول شما باید شامل سه بخش باشد

1. چشم انداز برنامه - جایی که می خواهیم باشیم
2. نتایج ارزیابی‌های بلوغ شما - جایی که در حال حاضر هستیم
3. تجزیه و تحلیل شکاف و اولویت های استراتژیک -چگونه به آنجا خواهیم رسید

یک چشم انداز برنامه امنیتی ایجاد کنید: برنامه های امنیت اطلاعات به یک چشم انداز واضح و مختصر نیاز دارند این بیانیه دستورات و اهداف سطح بالای امنیتی را بیان می کند. که باید با تیم، مدیریت و ذینفعان مربوطه به اشتراک گذاشته شود.

منابع برای مرحله طرح

برای شروع، منابع گارتنر زیر را مرور کنید.

تحقیق و ابزار گارتنر

راهنمای هیجانی در برنامه ریزی استراتژیک برای امنیت اطلاعات - با استفاده از راهنمایی های گام به گام ما یک برنامه استراتژیک ایجاد کنید.

بهترین روش‌های برنامه‌ریزی استراتژی امنیتی - یک برنامه استراتژیک عملی ایجاد کنید که برقرار شود.

اعتبار و ایجاد پشتیبانی

اولویت‌بندی پورتفولیوی امنیتی: افزودن سخت‌گیری به تصمیمات سرمایه‌گذاری امنیتی – طراحی یک روش تکرارپذیر و قابل دفاع برای اولویت‌بندی پروژه‌های امنیت داخلی.

جعبه ابزار: استراتژی امنیت اطلاعات در یک صفحه - ساختارشکنی شده - یک سند استراتژی یک صفحه ای ایجاد کنید که با رهبری C-suite همخوانی دارد.

مرحله عمل (هفته پنجم الی دوازدهم)

مرحله عمل بهبود قابلیت های امنیتی را ارائه می دهد. اقدامات درصد روزاول شما باید بر دستاوردهای ملموس و قابل مشاهده متمرکز باشد که اعتبار شخصی را ایجاد می کند و جایگاه امنیتی را در شرکت ارتقا می بخشد. موفقیت اولیه، خرید بیشتری را تضمین می کند، که از موفقیت بیشتر پشتیبانی می کند - بنابراین چرخه ای از پیشرفت و موفقیت را برای شما و تیمتان ایجاد می کند.

نتایج هدف برای مرحله قانون
در حین انجام اقدام، نتایج زیر را هدف قرار دهید:

- مجموعه ای از جلسات برنامه ریزی شده با مدیران امنیتی، کارکنان و تیم ها
- یک مالک پروژه اختصاص داده شده برای هر یک از اولویت های اصلی امنیت
- بودجه امنیتی که منابع کافی برای اولویت های استراتژیک شما را تضمین می کند
- فهرستی از نتایج ملموس و قابل اندازه گیری پروژه که نشان دهنده پیشرفت در برابر اهداف استراتژیک شما است

اقدامات برای مرحله قانون
هنگام اجرای طرح خود اقدامات زیر را انجام دهید:

نقش‌ها و مسئولیت‌ها را اصلاح کنید: اول، اطمینان حاصل کنید که همه مدیران امنیتی نقش‌ها و مسئولیت‌های مشخصی دارند. شفاف سازی کنید که هر مدیر امنیتی در قبال چه چیزی مسئول است و عملکرد آنها چگونه ارزیابی می شود. دوم، اطمینان حاصل کنید که همه کارکنان امنیتی در سطح خط شرح وظایف و مسئولیت های روشنی داشته باشید که به وضوح نشان دهنده کاری است که هر کارمند واقعا انجام می دهد. به خاطر داشته باشید که توصیف شغل و معیارهای مدیریت عملکرد اغلب با واقعیت های نحوه انجام کار متفاوت است - شکافی که باید تحت رهبری جدید شما اصلاح شود.

به یاد داشته باشید، مدیران امنیتی می توانند به توسعه نقش ها و مسئولیت ها برای خود و تیم هایشان کمک کنند. به عنوان CISO، شما باید بر این کار نظارت داشته باشید، اما احساس نکنید که باید تمام وظایف مدیریتی را خودتان انجام دهید.

واگذاری مالکیت پروژه: هر یک از اولویت های استراتژیک شما باید مدیر پروژه رسمی داشته باشد. یک برنامه، انتظارات و نتایج واضح برای هر پروژه ایجاد کنید و این موارد را با مدیران پروژه مشخص کنید. یکی از راه های به حداقل رساندن خطر شکست پروژه این است که اهداف چندگانه پروژه را تعیین کنید و از پروژه‌هایی که دارای نتایج باینری هستند (موفقیت یا شکست) اجتناب کنید.

پشتیبانی ایمن از رهبری: از برنامه استراتژیک و چشم انداز امنیتی خود برای مشارکت دادن رهبری و دریافت اولویت های اصلی خود استفاده کنید. پشتیبانی رهبری به شما و تیمتان دستوری می‌دهد که می تواند برای تأمین بودجه، تأثیرگذاری بر سهامداران و ایجاد انگیزه در تیم امنیتی استفاده شود.

ایجاد فرآیندها و انجمن های حاکمیتی امنیتی: شروع به کار برای ایجاد حاکمیت ریسک اطلاعات موثر در سراسر شرکت. این مستلزم حقوق تصمیم گیری ریسک، مسئولیت پذیری ریسک و مسئولیت های ذینفعان در سراسر شرکت برای ریسک اطلاعات یکی از بزرگترین چالش های شما به عنوان یک CISO جدید احتمالا القای مالکیت ریسک و تصمیم گیری مناسب است.

هرگونه تغییر بودجه لازم را اعمال کنید: در صورت لزوم، تغییرات بودجه را برای حمایت از اولویت های استراتژیک اولیه خود اعمال کنید. اولویت اصلی شما در حال حاضر اطمینان از بودجه و منابع کافی طی سه تا شش ماه آینده است. اکنون زمان خوبی برای شروع برنامه ریزی بودجه سال مالی آینده است. به عنوان یک CISO جدید، ممکن است حسن نیت و آزادی عمل قابل توجهی برای تخصیص مجدد بودجه یا حتی تامین منابع اضافی داشته باشید. به خاطر داشته باشید که بودجه اولیه شما احتمالاً به عنوان معیاری برای مقایسه در سال های آینده خواهد بود، بنابراین اطمینان حاصل کنید که بودجه خود را طوری ساختار می دهید که از یک نقشه راه چند ساله پشتیبانی کند.

ارتباطات در مرحله قانون

برنامه و چشم انداز استراتژیک خود را اجتماعی کنید: برنامه و چشم انداز استراتژیک خود را به رهبری و سهامداران در سراسر شرکت ارائه دهید. همانطور که برنامه خود را اجتماعی می کنید، با پیوند دادن برنامه خود به اولویت های ذینفعان، پیام خود را برای مخاطبان خود تنظیم کنید. ارتباط بین امنیت اطلاعات و اولویت ها و اهداف رهبران در سراسر سازمان را نشان دهید.

زمان‌بندی ورود به تیم و مدیر: مدیریت افراد یکی از جنبه‌های اصلی نقش CISO است. به عنوان اولین گام در مدیریت تیم خود، جلسات تکراری را در سراسر تیم امنیتی ایجاد کنید. به ویژه موارد زیر را در نظر بگیرید:

■ با هر یک از مدیران امنیتی چکهای هفتگی یک به یک انجام دهید. از این جلسات برای برنامه‌ریزی و پیگیری پروژه ها استفاده کنید. جلسات مدیر همچنین یک فرصت مربیگری است، به ویژه با توجه به القای آگاهی و زمینه تجاری در عملیات امنیتی روزمره.

■ "سطح رد شدن" ماهانه یا سه ماهه یک به یک با کارکنان امنیتی ایجاد کنید. می‌توانید این موارد را به‌صورت متوالی برنامه‌ریزی کنید تا هر هفته با چندین کارمند ملاقات کنید. این جلسات فرصتی برای برقراری ارتباط مستقیم با کارکنان، جمع آوری نظرات و سنجش روحیه است.

■ جلسات ماهانه همه دستی را برنامه ریزی کنید. به عنوان CISO، می توانیداعلامیه های مهمی را منتشرکنید، عملکردهای برتر را بشناسید و به روزرسانی های مهم را برای تیم کامل ارائه دهید. به عنوان یک فرصت توسعه، می توانید مدیران و کارکنان را برای ارائه دراین جلسات انتخاب کنید.

■ جلسات ایستاده تیم را تشویق کنید. مدیران امنیتی باید جلسات ثابت روزانه را با تیم های مربوطه خود درنظر بگیرند. این جلسات کوتاه (به عنوان مثال، کمتراز30 دقیقه) دستورکار روزرا تعیین می کند، فرصتی برای پرسش و پاسخ فراهم می کند و همکاری را تسهیل می کند. جلسات ایستاده روزانه مخصوصاً برای تیم‌های مجازی مهم است، زیرا آنها جایگزین مکالمات «کولرآبی» می‌شوند که دربین تیم‌های حضوری رخ می‌دهد.

منابع برای مرحله قانون
برای شروع، منابع گارتنرزیررا مرورکنید

تحقیق و ابزارگارتنر
مرکزپشتیبانی ارائه امنیت اطلاعات - ازالگوهای "دانلود و رفتن" برای تقویت پیام خود به رهبری و سهامداران در سراسرسازمان استفاده کنید.

ازابزارها و الگوهای مرتبط برای بلوغ فرآیندهای خود استفاده کنید:

■ راهنما برای توسعه یک طرح واکنش درحوادث امنیتی
■ راهنما برای طراحی و راه اندازی یک برنامه قهرمان امنیتی
■ راهنما برای برنامه ریزی استراتژیک برای امنیت اطلاعات
■ راهنما برای ایجاد یک داشبورد سلامت عملکردی برای امنیت اطلاعات
■ راهنما برای ایجاد یک برنامه آزمایش بحران سایبری

مرحله اندازه گیری (هفته یازدهم الی چهاردهم)

مرحله اندازه گیری شواهدی ازتأثیرشما برامنیت و شرکت ارائه می دهد. اندازه‌گیری و ارتباطات ازویژگی‌های بارز یک CISOموفق هستند، و شما باید درطول دوره تصدی خود تلاش قابل توجهی را به این مورد اختصاص دهید.

نتایج هدف برای مرحله اندازه گیری
هنگام سنجش عملکرد، نتایج زیررا هدف قراردهید:

■ مجموعه ای تعریف شده از معیارهای عملیاتی برای ردیابی عملکرد و پیشرفت در طرح های امنیتی.

■ شواهدی از پیشرفت اولیه که باید به ذینفعان و تیم رهبری گزارش شود.

■ تشکیل جلسه و برنامه گزارش دهی برای ذینفعان مختلف، از جمله CIO، کمیته راهبری ریسک، C-suiteو هیئت مدیره

اقدامات برای مرحله اندازه گیری
مجموعه ای از معیارهای امنیتی را تعریف کنید: مجموعه کوچکی از KPIهای عملیاتی ایجاد کنید و سپس این معیارهای عملیاتی را با معیارهای مرتبط با کسب و کار که با رهبری و هیئت مدیره طنین انداز می شود، تطبیق دهید. بهترین معیارهای مربوط به کسب و کار شامل زمینه کسب و کار و به دور از جزئیات فنی است.

توسعه یک فرآیند گزارش‌دهی اجرایی: تعداد دفعات گزارش‌دهی و مخاطبان، مانند کمیته‌های راهبری، جلسات توجیهی C-suiteو گزارش‌های هیئت مدیره (کمیته کامل و ریسک) را ایجاد کنید. پس از تنظیم انتظارات گزارش، زمانی را صرف درک انتظارات و اولویت های هر مخاطب کنید. سپس، معیارها و گزارش‌های مربوط به هر مخاطب را ایجاد کنید و فرآیندها و مسئولیت‌هایی را برای کارکنان امنیتی ایجاد کنید تا این داشبوردها را به‌طور منظم نگهداری و به‌روزرسانی کنند.

ارتباطات در مرحله اندازه گیری
نظارت بر پیشرفت برنامه و پروژه: پیشرفت امنیت و دستاوردهای بلوغ برنامه را دنبال کنید. پیشرفت را به رهبری گزارش دهید، و از این حرکت برای ایجاد شرایط تجاری برای ادامه (یا افزایش) بودجه و حمایت در صورت نیاز استفاده کنید. مدیران امنیتی و رهبران پروژه برای بیان امنیت در شرایط مرتبط با تجارت. تیم رهبری شما باید بتواند به طور مختصر توضیح دهد که چگونه اولویت های امنیتی به اهداف تجاری شرکت نگاشته شده و از آنها پشتیبانی می کند.

برنده‌ها و چالش‌های اولیه را برجسته کنید: با برقراری ارتباط با برنده‌ها و شناسایی راه‌حل‌هایی برای رسیدگی به چالش‌ها به محض ظهور، حرکت خود را حفظ کنید. به خاطر داشته باشید که بیشتر ابتکارات امنیتی اهداف متعددی دارند (برخی کوچکتر، برخی بزرگتر) و حتی اگر برخی از اهداف به تعویق افتاده یا از دست رفته، برخی دیگر ممکن است به دست آیند.

منابع برای مرحله اندازه گیری
برای شروع، منابع گارتنر زیر را مرور کنید

تحقیق و ابزارگارتنر
چرا باید یک کارت امتیازی متوازن برای مدیریت امنیت و ریسک ایجاد کنید - یک کارت امتیازی متوازن برای انتقال معیارهای مربوط به کسب و کار به رهبری پیاده‌سازی کنید.

جعبه ابزار: توسعه یک کارت امتیازی متوازن برای امنیت - از این ابزار دانلود و رفتن برای ایجاد سریع کارت امتیازی متوازن امنیتی استفاده کنید.

پنج ویژگی مورد نیاز معیارهای امنیتی - معیارهایی را طراحی کنید که بهترین شیوه ها را برآورده کنند.

ابزار: یک داشبورد مدیریتی ساده - یک داشبورد مدیریت امنیتی ایجاد کنید که استانداردهای صنعت را منعکس کند به عنوان مثال، چارچوب امنیت سایبری NIST و با رهبران ارشد در سراسر سازمان به اشتراک گذاشته شود.

تاریخچه ویرایش سند
صد روز اول افسر ارشد امنیت اطلاعات - 27 ژوئن 2014
صد روز اول حیاتی CISO جدید - 17 فوریه 2011
جعبه ابزار: صد روز اول حیاتی CISO جدید - 2 فوریه 2007

توصیه شده توسط نویسندگان
ممکن است برخی از اسناد به عنوان بخشی از اشتراک فعلی گارتنر شما در دسترس نباشند.
نقشه راه برای اثربخشی CISO
بهترین شیوه های برنامه ریزی استراتژی امنیتی
امتیازفناوری اطلاعات برای مدیریت امنیت و ریسک
پنج سوال هیئت مدیره که رهبران امنیت و ریسک باید آماده پاسخگویی باشند

هدف	فاز
برای نقش خود قبل از روز اول برنامه ریزی کنید	آماده کردن
بلوغ فعلی اوراق بهادار را درک کنید	ارزیابی کنید
یک نقشه راه برای صد روز اول ایجاد کنید	طرح
بهبودهای بلوغ قابل مشاده را اعمال کنید	عمل کنید
شواهدی از پیشرفت امنیت ارائه دهید	اندازه گرفتن

Gartner

بینش عملی و عینی

اطمینان حاصل کنید که عملکرد امنیت سایبری شما برای موفقیت در موقعیتی قرار دارد. این منابع و ابزارهای اضافی برای امنیت و رهبران ریسک کاوش کنید:

Infographic

Protect Your Business Assets With a Roadmap for Maturing Information Security Program

Make sure your security adapts to current and new threats.

Download Infographic

eBook

3 Must-Haves in Your Cybersecurity Incident Response

Build a cybersecurity response plan for your organization today.

Download Now

Research

Predicts 2022: Cyber-Physical Systems Security — Critical Infrastructure in Focus

Prepare your enterprise for a secure future.

Download Now

Webinar

The Gartner Leadership Vision for 2022: Security and Risk Management

Plan for 2022 and stay ahead of the evolving challenges.

Watch On Demand

Gartner

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 دارایی‌های دیجیتال سازمان‌ها می‌باشد. در تلاش هستیم با خدمات مشاوره، اجرا، پیاده‌سازی و راهبری پروژه‌ها 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 بهره‌وری و ارزش آفرینی می‌پردازیم.

شعار شرکت:
"سپر امنیتی ما، همراهی قدرتمند برای آینده‌ی شما"

www.csdpc.ir
info@csdpc.ir

Gartner