نمونه سوالات امتحانی
درس مدیریت شبکه وامنیت درفضای تبادل داده

دوره Ph.D رشته مدیریت فناوری اطلاعات

استاد: دکتر بازایی

دی ماه ۱۳۹۶

۱. مثلث CIA چه اهمیتی دارد؟ هر یک از اضلاع آن را به اختصار توصیف کنید

اهمیت آن در قابلیتش در توسعه جامع مجموعه ای از ویژگی ها و فرایندهای حیاتی امنیت است.

الف) محرمانگی: یکی از مشخصه های اطلاعات است که فقط کسانی با صلاحیت و اختیارات مشخص می توانند به آن دسترسی داشته باشند. هنگامی که افراد یا سیستم های غیر مجاز بتوانند اطلاعات محرمانه ای را مشاهده کنند، محرمانه بودن نقض می شود.

ب) یکپارچگی: به طور کلی یکپارچگی یعنی کیفیت یا وضعیت کلی، کامل و بدون آسیب و هر نوع آسیب، تخریب و یا اختلال در این کل یک تهدید به حساب می آید.

ج) دسترسی: این امر زمانی اتفاق می افتد که کاربران بدون دخالت و هر نوع محدودیتی قادر به استفاده از اطلاعات باشند. در دسترس بودن به این معنی نیست که اطلاعات در اختیار هر کاربر قرار گیرد، بلکه به معنی دسترسی کاربران مجاز به اطلاعات می باشد.

۲. تعریف "حریم خصوصی" با توجه به مبحث امنیت اطلاعات چیست؟ این تعریف چه تفاوتی با تعاریف دیگر دارد؟

حریم خصوصی بدین معناست که اطلاعات مربوطه تنها به شیوه ای که مورد تایید فرد تهیه کننده آنها است، باید مورد استفاده قرار گیرد. در تعاریف دیگر حریم خصوصی معادل آزادی در مشاهده و رصد کردن می باشد، در حالی که در تعریف فوق نه تنها این امر مورد تایید نمی باشد، بلکه شیوه ملاحظه و استفاده توسط مالک اطلاعات تعیین می شود و حتی با وجود دسترسی داشتن و استفاده از چندین منبع مختلف نیز امکان استفاده از اطلاعات خصوصی افراد وجود ندارد.

۳. ساختار تفکیک کار (WBS) چیست و چرا اهمیت دارد؟

اساس روش "ساختار تفکیک کار" در تقسیم پروژه به چندین وظیفه اصلی همچون الف) میزان کار انجام شده، ب) مهارت های رایج یا تخصصی مورد نیاز برای انجام کار، ج) مقدار زمان تخمینی مورد نیاز برای انجام هر کار و ... و تقسیم هر چه بیشتر آن به وظایف کوچک تر و یا اقدامات خاصی می باشد.

اهمیت این روش در این است که در یک پروژه واقعی، وظایف اغلب پیچیده هستند. در نتیجه ساده سازی و تقسیم مشخص و اختصاص داده شده مراحل کار یک گام عملی است که می تواند توسط یک فرد یا یک مجموعه مهارت تکمیل شود و تا زمانی که نتیجه تکمیل شود.

۴. برنامه ریزی راهبردی از بالا به پایین را توضیح دهید؟ این نوع برنامه ریزی چه فرقی با برنامه ریزی از پایین به بالا دارد؟

برنامه ریزی استراتژیک، مسیر حرکت طولانی مدت سازمان را مشخص می کند.راهبرد از بالا به پایین، رویکردی سیستماتیک است و در بالاترین سطوح سازمان تشکیل و به برنامه های راهبردی مشخص تر برای لایه های

مدیریت متوسط تبدیل می شود. این برنامه ها، به برنامه ریزی تاکتیکی برای مدیران نظارتی تبدیل و در نهایت جهت برنامه های عملیاتی برای رده فنی سازمان ارائه می شود. ای نوع برنامه ریزی از پشتیبانی حداکثری مدیریت ارشد برخوردار است و اغلب امکانات مالی، برنامه ریزی روشن، موفقیت در روند پیاده سازی و قابلیت توانایی نفوذ در فرهنگ سازمانی را دارا می باشد.

موفق ترین نوع این رویکرد شامل یک استراتژی توسعه رسمی به نام چرخه عمر توسعه سیستم (SDLC) است.

همچنین برای موفقیت در این راهبرد، مدیریت ارشد باید حمایت کامل تمامی بخش ها را بدست آورد. در این خصوص بعضا وجود و حضور یک قهرمان، همچون یک مدیر اجرایی با نفوذ کافی برای حرکت دادن پروژه به جلو و مطمئن شدن از درستی شیوه های مدیریتی در سراسر سازمان، ضروری است.

تفاوت اصلی راهبرد پایین به بالا با بالا به پایین در این است که این رویکرد به ندرت کار می کند، چرا که برخی از ویژگی های حیاتی مانند برنامه ریزی هماهنگ شده از اداره عالی، هماهنگی بین ادارات و تأمین منابع کافی، برخوردار نیست.

۵. در بحث امنیت اطلاعات، "تهدید" به چه معنا می باشد؟ انواع تهدید را نام ببرید.

تهدید به معنای برنامه و حرکتی برای خرابی و یا دزدی اطلاعات و یا اموال فیزیکی یک سازمان می باشد.

۱) جاسوسی، ۲) نیروهای طبیعی، ۳) خطا یا قصور انسانی، ۴) اخاذی اطلاعاتی، ۵) خرابکاری، ۶) حملات نرم افزاری، ۷) نقص یا خطای فنی سخت افزاری، ۸) نقص یا خطای فنی نرم افزاری، ۹) قدیمی شدن فناوری، ۱۰) دزدی

۶. نقاط آسیب پذیر چگونه مورد حمله قرار می گیرند؟

آسیب پذیری به معنای وجود یک نقطه ضعف در درون یک دارایی اطلاعاتی مورد مراقبت می باشد که اغلب نتیجه عدم مراقبت کافی می باشد. عمدتا شوق رسوخ به درون سیستم ها و امکان بهره برداری از این نقاط آسیب پذیر باعث انجام اقداماتی منجر به حمله می شود.

۷. مراحل هفت گانه مورد پیشنهاد بنیاد ملی استاندارد و فناوری (NIST) در برنامه ریزی احتمالی (CP) را توضیح دهید؟

- توسعه خط مشی "برنامه ریزی احتمالی": نگارش خط مشی رسمی در راستای ایجاد روند یک برنامه احتمالی موثر و مقتدر
- پیاده سازی "تجزیه و تحلیل تاثیر کسب و کار" (BIA): "تجزیه و تحلیل تاثیر کسب و کار" به شناسایی و اولویت بندی سیستم های اطلاعات و اجزای حیاتی پشتیبان فرایندهای ماموریتی / کسب و کاری سازمان، کمک می کند.

- شناسایی کنترل های پیشگیرانه: اقدامات انجام شده برای کاهش اثرات خرابی های سیستم می تواند باعث افزایش دسترسی به سیستم و کاهش هزینه های چرخه زندگی احتمالی شود.
- خلق راهبردهای احتمالی: راهبردهای کامل جبرانی، اطمینان بخش بهبود سریع و موثر سیستم های مورد اختلال قرار گرفته می باشند.
- توسعه طرحی احتمالی: این طرح احتمالی باید حاوی دستورالعمل های دقیق برای بازسازی امکانات سازمانی آسیب دیده درهر سطح از واحد کسب و کار باشد.
- اطمینان از تست، آموزش لازم جهت برنامه: تست تأیید توانایی های بازیابی را در بر می گیرد، در حالی که آموزش کارکنان بازیابی را برای فعال سازی برنامه آماده می کند و برنامه ریزی را مشخص می کند.
- اطمینان از نگهداری برنامه: این طرح باید یک سند زنده که به طور منظم به روز می شود، باشد تا با پیشرفت های سیستم و تغییرات سازمانی باقی بماند.

۸. اصطلاح "حادثه" در برنامه ریزی پاسخ به حادثه (IRP) چه می باشد؟ چه ارتباطی با مفهوم پاسخ به حادثه دارد؟

در "برنامه ریزی پاسخ به حادثه" یک رویداد غیر منتظره را حادثه می نامند. "پاسخ به حادثه" شامل مجموعه ای از رویه ها که در صورت شناسایی یک حادثه، شروع به عمل می کنند.

۹. برنامه ریزی تداوم کسب و کار (BCP) چیست و چرا اهمیت دارد؟

برنامه ریزی تداوم کسب و کار(BCP) ، طرحی است که در صورت وقوع رخدادی غیر منتظره و یا فاجعه ای بزرگ، عملکرد های مهم و اساسی سازمان از کار نیفتاده و قادر به ادامه مسیر باشند. اهمیت آن در مدیریت کامل فرایند توسط مدیریت ارشد (مدیرعامل) سازمان است و اینکه بیشتر به بازسازی وظایف حیاتی تجاری و نه زیرساخت های فنی کسب و کار بر می گردد.

۱۰. مدل چشم گاو (به اصطلاح: قلب هدف هم گفته می شود) را توضیح دهید؟ لایه خط مشی را توضیح دهید؟

مدل چشم گاو، یک مدل اجرایی مبتنی بر اهمیت نقش خط مشی در برنامه امنیت اطلاعات می باشد. از آنجا که این مدل یک مکانیسم اثبات شده برای اولویت بندی تغییرات پیچیده فراهم می کند، به طور گسترده ای در میان متخصصین امنیت اطلاعات پذیرفته شده است. در این مدل، با توجه به حرکت مسائل از کل به خاص، همیشه خط مشی آغازگر مدل می باشد یعنی، تمرکز بر روی راه حل های سیستمیک به جای مشکلات فردی است. این مدل شامل چهار لایه: ۱) خط مشی ها، ۲) شبکه ها، ۳) سیستم ها و ۴) برنامه های کاربردی است.

خط مشی، بیرونی ترین لایه در مدل چشم گاو و منعکس کننده دیدگاه اولیه اکثر کاربران برای تعامل با امنیت اطلاعات است. خط مشی به عنوان یک سند بالادستی منتشر می شود و بیان کننده اراده مدیریت و هدایت کننده

رفتار کاربران است.

۱۱. هدف "خط مشی مسائل امنیتی خاص" (ISSP) چیست؟

هدف این خط مشی رسیدن به درکی مشترک از منابعی است که یک کارمند مجاز به استفاده از آن است، می باشد. هنگامی که این درک برقرار شد، کارکنان قادر هستند بدون هرگونه تاییدی از منابع استفاده نمایند. این نوع از خط مشی اعمال می شود تا هم کارکنان و هم سازمان را از ناکارایی و ابهام حفظ نماید.

۱۲. چهار عنصر موجود در "خط مشی اطلاعات امنیت شرکت" (EISP) را توضیح دهید؟

- بررسی اجمالی فلسفه امنیتی شرکت
- داشتن اطلاعات در خصوص ساختار مدیریت امنیت اطلاعات، افراد و پست های موجود در این مدیریت
- مسئولیت های امنیتی کاملا مشخص و مشترک در همه اعضای سازمان (کارکنان، پیمانکاران، مشاوران، شرکا و بازدیدکنندگان)
- مسئولیت های امنیتی کاملا مشخص و خاص برای هر پست در سازمان

۱۳. وظایف مدیریت امنیت اطلاعات به چند بخش تقسیم می شوند؟ توضیح دهید.

به ۴ بخش تقسیم می شود.

- وظایفی که توسط واحدهای غیر فنی کسب و کار و خارج از محدوده فناوری مدیریت کنترل همچون: حقوق و آموزش انجام می شوند.
- وظایفی که توسط گروه های فناوری خارج از محدوده مدیریت کنترل امنیت اطلاعات همچون مدیریت امنیت شبکه، احراز هویت مرکزی و ... انجام می شوند.
- وظایفی که مدیریت امنیت اطلاعات به عنوان خدمات مشتری به سازمان و شرکای خارجی اش ارایه می دهد. همچون ارزیابی خطر، تست سیستم ها، برنامه ریزی و ...
- وظایفی که به عنوان وظایف ذاتی و اجرایی مدیریت امنیت اطلاعات انجام می شوند. همچون خط مشی گذاری، مطابق/ممیزی و مدیریت ریسک

۱۴. طبقه بندی سه گانه موقعیت های امنیت اطلاعات را نام برده و هر یک را مختصرا توضیح دهید؟

- کسانی که تعریف می کنند: این افراد راهبردها کلان و خط مشی ها رو نوشته و مشخص می کنند.
- کسانی که مدیریت می کنند: این دسته جزو مدیران میانی و تاکتیکی بوده و بر عملکردهای میانی و اجرایی سازمان نظارت دارند.
- کسانی که می سازند: این دسته جز فن سالاران، طراحان و کارگران می باشند که بر اساس نیاز می توانند آموزش های لازم را هم ببینند.

۱۵. طرح بلوپرینت امنیت اطلاعات چیست؟

طرح بلو پرینت امنیت اطلاعات کنترل های موجود را توصیف و سایر کنترل های امنیتی لازم را شناسایی می کند. این طرح در اکثر سازمان ها بر اساس مدل ها و رویکردهای امنیتی شان رسم می شود.

۱۶. کنترل دسترسی چیست؟

این امر به معنای کنترل دسترسی منطقی کاربران قابل اعتماد به سیستم های اطلاعاتی و امکانات فیزیکی سازمان می باشد. کنترل دسترسی با استفاده از مجموعه ای از خط مشی ها، برنامه های اجرایی و فناوری هایی که این خط مشی ها را اجرا می کنند، قابل اعمال کردن می باشد.

کنترل دسترسی به طور کلی شامل چهار فرآیند است: دستیابی به هویت نهادی که درخواست دسترسی به یک محدوده نرم افزاری یا فیزیکی را دارد (شناسایی)؛ تأیید هویت نهادی که به دنبال دستیابی به محدوده نرم افزاری یا فیزیکی است (احراز هویت)؛ تعیین میزان دسترسی نهاد مذکور به محدوده نرم افزاری و یا فیزیکی (مجوز) و در نهایت مستند سازی فعالیت های افراد و سیستم های مجاز (مسئولیت پذیری).

کنترل دسترسی، سازمان ها را قادر می سازد تا دسترسی به اطلاعات، دارایی های اطلاعاتی و سایر دارایی های ملموس را به افراد مجاز واقعی آن کسب و کار محدود کنند.

۱۷. COBIT چیست؟

COBIT نوعی چارچوب کسب و کار برای راهبرد و مدیریت یک شرکت فناوری اطلاعات می باشد. آخرین نسخه این مدل شامل آخرین تفکرات در حوزه راهبری و فنون مدیریت شرکت ها، اصول پذیرفته شده جهانی، رویکردها، ابزار و مدل های تجزیه و تحلیل در جهت کمک به افزایش اعتماد به سیستم های اطلاعاتی می باشد.

۱۸. رویکرد پایه ایی (Baselining) چیست؟

رویکرد پایه ایی، رویکردی مرتبط با معیار سنجش است که بر اساس یک ارزیابی قبلی یا یک هدف داخلی اندازه گیری می شود. این رویکرد، ارزیابی عملکرد برخی از اقدامات یا فرآیند را انجام می دهد. این اندازه گیری عملکرد (که گاهی اوقات به عنوان معیار عملکرد نامیده می شود) می تواند برای مقایسه عملکرد فعلی در برابر یک مقدار مشاهده شده پیشین یا مقدار مورد نظر برای آن عمل یا فرآیند مورد استفاده قرار گیرد. بنابراین، رویکرد پایه ایی، فرایند اندازه گیری در برابر یک ارزش یا استاندارد داخلی است.

۱۹. عوامل حیاتی در موفقیت اجرای یک برنامه امنیت اطلاعات چیست؟

- پشتیبانی قوی مدیریت ارشد: این مهم نه تنها برای موفقیت برنامه بلکه برای اجرای برنامه نیز لازم است.
- رویه های و خط مشی های عملی امنیت اطلاعات: باید ساختار مدیریت امنیت اطلاعات مشخص و مسئولیت های کلیدی شناسایی شوند.

- میزان های قابل اندازه گیری عملکرد: این مورد برای ضبط و ارائه داده های عملکرد معنی دار طراحی شده است. بر اساس اهداف عملکردی امنیت اطلاعات، میزان های عملکرد باید به راحتی قابل دستیابی و اجرا باشند.
- تجزیه و تحلیل میزان نتایج: این عامل برای استفاده از درس های یاد گرفته شده، بهبود کارایی کنترل های امنیتی موجود و برنامه ریزی برای اجرای کنترل های امنیتی آینده و برای برآورده شدن نیازهای جدید امنیت اطلاعات مورد استفاده قرار گیرد.

۲۰.سه محدوده اجرایی برنامه SETA رو نام ببرید؟

- تحصیلات در حوزه امنیت،
- آموزش موارد امنیتی،
- آگاهی رسانی در خصوص مباحث امنیتی

۲۱.اعتباربخشی سیستم چیست؟

در مدیریت امنیت، اعتباربخشی، مجوز یک سیستم فناوری اطلاعات برای پردازش، ذخیره و یا انتقال اطلاعات است. اعتباربخشی توسط مدیریت ذی صلاح صادر و به عنوان وسیله ای برای اطمینان حاصل کردن از کیفیت مناسب سیستم ها عمل می کند. همچنین با ایجاد چالش در بین مدیران و کارکنان فنی، سعی در یافتن بهترین روش ها با توجه به محدودیت های فنی، عملیاتی و نیازهای ماموریت دارد.

۲۲.کدوم یک از خصوصیات اطلاعات هیچگاه در عناصر نرم افزاری اعمال نمی شود ؟

موقعیت فیزیکی. با این وجود، برخی از سازمانها ممکن است مجوزی داشته باشند که نشان دهد از کدام نرم افزار میتواند استفاده کرد. این ممکن است شامل سیستم های اجاره شده در نقاط دور افتاده (به اصطلاح "تجهیزات مشترک")، که اغلب به عنوان "در ابر" توصیف می شود، نیز شود.

۲۳.صفحه کاری TVA را شرح دهید و کاربرد آن را بگویید؟

در پایان روند شناسایی ریسک، یک سازمان باید فهرست اولویت دارایی ها و آسیب پذیری های آخود را داشته باشد. این لیست به عنوان نقطه شروع برای مرحله بعدی فرایند مدیریت ریسک یعنی ارزیابی خطر است. همچنین لیست دیگری تهدیدات سازمان را بر اساس جدول وزنی مورد بحث قرار می دهد. این دو لیست می تواند در یک صفحه کاری با عنوان تهدیدات، آسیب پذیری، دارایی ها (TVA) ترکیب شوند. در محور افقی دارایی ها با اولویت از چپ به راست قرار می گیرند و در محور عمودی تهدیدات با اولویت از بالا به پایین قرار دارد.
نتیجه، این شبکه، ایجاد روشی مناسب برای بررسی "قرار گرفتن" دارایی ها و امکان ارزیابی آسیب پذیری ساده را فراهم می کند.

۲۴. آسیب پذیری چیست؟

راه های خاصی هستند که عوامل تهدید جهت حمله به یک دارایی اطلاعاتی از آنها سوء استفاده می کنند. به عبارت دیگر، آنها به عنوان شکاف هایی در زره های دارایی ها هستند مواردی همچون نقص یا ضعفی در رویه، طراحی یا کنترل امنیتی یک دارایی اطلاعاتی که می تواند به صورت تصادفی یا به طور هدفمند مورد سوء استفاده قرار گیرند تا امنیت را نقض کند.

۲۵. راهبردهای پنجگانه کنترل ریسک را بیان کنید؟

- دفاع: اعمال حفاظتی که خطر ریسک کنترل نشده را از بین می برد یا کاهش می دهد
- انتقال: انتقال خطرات به محدوده های دیگر و یا اشخاص خارجی
- کاهش: کاهش تاثیرات دارایی های اطلاعاتی به گونه ای که یک مهاجم قادر به بهره برداری کامل از یک آسیب پذیری نباشد.
- پذیرش: درک عواقب حاصل از انتخاب ریسک بدون کنترل و تصدیق درستی ریسک بدون هرگونه تلاشی در کنترل آن
- فسخ: حذف یا متوقف کردن دارایی اطلاعات از محیط عملیاتی سازمان.

۲۶. آنالیز هزینه – فایده چیست؟

معیاری که بیشترین استفاده را در ارزیابی راهبردها برای کنترل و محافظت امنیت اطلاعات دارد، امکان سنجی اقتصادی است. این بدین معناست که هر یک از گزینه ها ممکن است یک مشکل خاص را حل کنند، اما برخی از آنها گران تر از دیگران هستند. سازمان ها می توانند این نوع تجزیه و تحلیل امکان سنجی اقتصادی را با ارزیابی دارایی های اطلاعاتی و تعیین ضرر ارزش در صورت مواجه شدن با این دارایی های اطلاعات شروع کنند.

این فرآیند تصمیم گیری، یک تجزیه و تحلیل هزینه–سود (CBA) یا یک مطالعه امکان سنجی اقتصادی است که در آن همانطور که تعین هزینه ارزش اطلاعات سخت می باشد، تعیین هزینه های حفاظت نیز دشوار است. همچنین فایده، ارزش سازمان برای استفاده از کنترل ها جهت جلوگیری از تلفات مربوط به یک آسیب پذیری خاص است.

در این آنالیز، معمولا ارزش دارایی های اطلاعاتی یا آنهایی که در معرض آسیب پذیری هستند تعیین می شود، آنگاه ارزش آن بخش از دارایی ها که در معرض خطر هستند مشخص می شود و در انتها میزان ریسک موجود دارایی مشخص می گردد.

۲۷. شیوه های OCTAVE چیست؟ چه کسی آن را به کسانی که آن را اتخاذ می کنند ارائه می دهد؟

روش ارزیابی تهدیدات حیاتی عملیاتی، دارایی و آسیب پذیری (OCTAVE)، یک روش ارزیابی ریسک امنیت

اطلاعات است که به سازمان ها اجازه می دهد تا بین دارایی های اطلاعات حیاتی خود و هزینه های کنترل های امنیتی تعادل ایجاد کند. این فرایند سازمان را قادر به اندازه گیری خود در برابر رویکردهای امنیتی خوب شناخته شده یا پذیرفته شده می نماید. این امر منجر به ایجادراهبردی حفاظتی برای کل سازمان و برنامه کاهش مخاطرات توسط امنیت اطلاعات می شود.

۲۸. چه تفاوتی بین "احراز هویت" و "مجوز" می باشد؟ چرا سیستم نمی تواند "مجوز" بدون "احراز هویت" صادر کند؟

"احراز هویت" به معنای تأیید هویت نهادی است که خواستار دسترسی به یک محدوده نرم افزاری یا فیزیکی است در حالیکه "مجوز" به معنای تعیین اقدامات و میزان دسترسی که نهادها می توانند در محدوده نرم افزاری یا فیزیکی داشته باشند، است. به دلیل تقدم و تالی بودن احراز هویت و مجوز، نخست باید موجودیت فرد یا نهاد مشخص و تایید شد، آنگاه به هویت مورد تایید امکان و مجوز دسترسی به محدوده اطلاعات را داد. به دلیل ارتباط ترتیبی این دو موضوع، سیستم قادر به صدور مجوز بدون احراز نمی باشد.

۲۹. RADIUS چیست؟

سیستم اعتبار سنجی از راه دور (RADIUS) سیستمی است که مدیریت تأیید هویت کاربران را با قرار دادن مسئولیت تأیید اعتبار هر کاربر در یک سرور مرکزی متمرکز می نماید. هنگامی که یک سرور دسترسی از راه دور (RAS) درخواستی برای اتصال شبکه از یک سرویس گیرنده Dial-up دریافت می کند، درخواست را همراه با اعتبار کاربری کاربر به سرور RADIUS می فرستد. RADIUS پس از تایید اعتبار، تصویب تصمیم (قبول یا رد) را به RAS منتقل می کند.

۳۰. چه نوع داده و اطلاعاتی با استفاده از پکت اسنیفر کشف می شود ؟

پکت اسنیفر یکی از ابزار شبکه است که کپی پکت های حاصل از شبکه را جمع آوری و تجزیه و تحلیل می نماید.

۳۱. چه عواملی در انتخاب و استخدام پرسنل امنیت اطلاعات موثر هستند؟

- داشتن درک صحیح از ساختار و نحوه راهبری سازمان
- داشتن در ک صحیح از اینکه امنیت اطلاعات امری مدیریتی است که فقط با تکنولوژی همراه نمی باشد.
- قابلیت برقرار ارتباط خوب با افراد از جمله کاربران به همراه داشتن مهارت های قوی کلامی و نوشتاری
- آگاهی داشتن در خصوص نقش خط مشی سازمان در به ثمر رسیدن اطلاعات
- درک وجود تحصیلات و آموزش های مرتبط در خصوص نقش های اصلی امنیت اطلاعات که کاربر را به عنوانی جزئی از راه حل و نه مشکل ببینند.

- داشتن درک صحیح از تهدیدات یک سازمان، چگونگی تبدیل این تهدیدات به حملات و حفاظت سازمان از دست این گونه حملات
- داشتن درک صحیح از نحوه کنترل فنی (از جمله فایروال ها، سیستم های تشخیص نفوذ و نرم افزار آنتی ویروس) که می تواند برای حل مشکلات خاص امنیت اطلاعات استفاده شود.

۳۲. خط مشی چیست؟ مهمترین تفاوت آن با قانون در چیست؟

اکثر سازمان ها شرح و توصیف رفتار کارمند قابل قبول و غیر قابل قبول را زیر مجموعه خط مشی شرح می دهند. خط مشی های تعریف شده و به درستی اجرا شده در یک سازمان همچون شیوه مجازات ها، اقدامات قضایی و تحریم ها عمل می کنند. از آنجاییکه خط مشی ها مانند قوانین عمل میکنند، باید مشابه آنها در نظر گرفته شده شده و اطمینان حاصل شود که این خط مشی ها برای همه پرسنل موجود در محل کار به شکلی کامل، مناسب و عادلانه اعمال می شود.

تفاوت اصلی خط مشی و قانون در این است که نادیده گرفتن خط مشی، یک دفاع قانونی است.

۳۳. بهترین شیوه جلوگیری از رفتارهای غیرقانونی و غیر اخلاقی چیست؟

بازدارندگی بهترین روش برای جلوگیری از فعالیت غیر قانونی یا غیر اخلاقی است. قوانین، سیاست ها و کنترل های فنی همه نمونه هایی از بازدارنده ها هستند. با این حال، قوانین و سیاست ها و مجازات های مرتبط با آن فقط در صورتی که سه شرط زیر وجود داشته باشد می تواند مانع شود:

- ترس از مجازات: تهدید غیر رسمی یا هشدارهای کلامی ممکن است تاثیر مشابهی چون تهدید به حبس یا جبران خسارت نداشته باشد.
- احتمال دستگیری: وجود این احتمال که عاملان اقدامات غیرقانونی یا غیر اخلاقی حتما دستگیر خواهند شد.
- احتمال وقوع مجازات: سازمان باید مایل و مجاز به اعمال مجازات باشد.

پایان