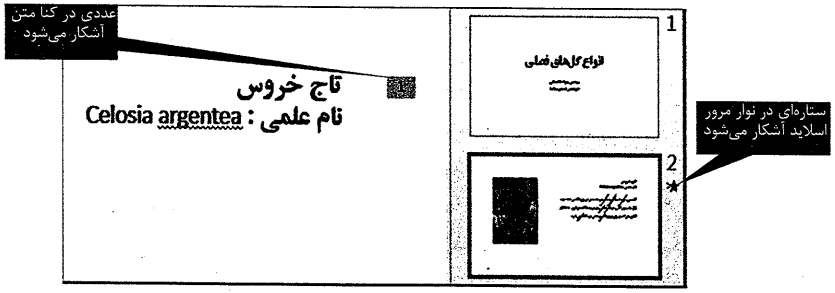
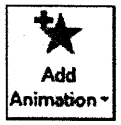


شکل ۸ـ۱۶ عدد و ستاره نشان می‌دهند که شیئی انیمیشن شده است.

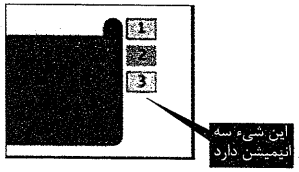
۸ـ۳۵ـ۱ افزودن چند پویانمایی به یک شیء



می‌توان به یک شیء چند پویانمایی افزود. مرحله‌های زیر را انجام دهید:

۱. شیء مورد نظر را برگزینید. در ریبون صفحهٔ Animations را کلیک کنید.

۲. در گروه Advanced Animation، گزینهٔ Add Animation را کلیک کنید. لیستی از پویانمایی موجود نمایش داده می‌شود.



۳. پویانمایی دلخواه را کلیک کنید.

اگر شیئی بیش از یک پویانمایی داشته باشد، برای هر پویانمایی یک شمارهٔ جداگانه در کنار آن آشکار می‌شود. این شماره‌ها ترتیب اجرا شدن پویانمایی‌ها را نشان می‌دهند.

۸ـ۳۵ـ۲ کپی کردن پویانمایی

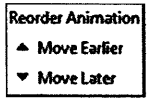
گاهی لازم است که افکت‌های یک شیء را به شیء دیگری اعمال کنید. می‌توانید افکت‌ها را توسط Animation Painter کپی کنید. مرحله‌های زیر را انجام دهید:

۱. در یک اسلاید، شیء دارای افکت را کلیک کنید.

۲. در ریبون، در صفحهٔ Animations، گزینهٔ Animation Painter را کلیک کنید.

۳. شیئی که می‌خواهید افکت‌ها به آن کپی شود را برگزینید. افکت‌ها به این شیء اعمال می‌شوند.

۸ـ۳۵ـ۳ تغییر دادن ترتیب اجرای پویانمایی



اگر شیئی بیش از یک پویانمایی دارد، می‌توانید ترتیب اجرای پویانمایی‌های آن را معین کنید.

۱. عدد مربوط به افکت را کلیک کنید.

۲. در صفحهٔ Animations، در گروه Timing، دستور Move Later یا Move Earlier را کلیک کنید.

۸ـ۳۵ـ۴ نمایش پویانمایی

هر پویانمایی که اعمال کنید، هنگام پخش اسلایدها نمایش داده می‌شوند. برای دیدن پیش‌نمایشی از پویانمایی اعمال‌شده، مرحله‌های زیر را انجام دهید:

۱. اسلاید دارای پویانمایی را کلیک کنید.

۲. در صفحهٔ Animations، درگروه Preview، گزینهٔ Preview را کلیک کنید.

۸ـ۳۵ـ۵ حذف پویانمایی

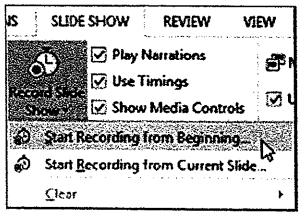
برای حذف یک پویانمایی از روی یک شیء، مرحله‌های زیر را انجام دهید:

۱. عدد کوچکی که در کنار شیء پویانمایی‌شده قرار دارد را کلیک کنید.

۲. کلید Delete صفحه‌کلید را فشار دهید.

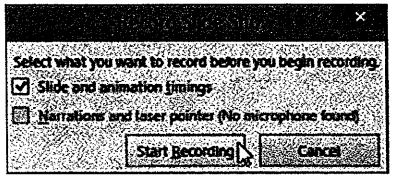
۸ـ۳۶ ضبط کردن نمایش اسلایدها

هنگام نمایش اسلایدها می‌توانید آنها را ضبط کنید. اگر میکروفن دارید، می‌توانید صدایی را روی کل نمایش ضبط کنید. اشاره‌گر موشی یا ماوس در اسلایدهای ضبط‌شده نشان داده نمی‌شود. اگر می‌خواهید در هنگام ضبط، جزئیات صفحه را با اشاره‌گر نشان دهید، باید از گزینهٔ Laser Pointer استفاده کنید. برای ضبط نمایش، مرحله‌های زیر را انجام دهید:



۱. یک نمایش را باز کنید، در ریبون، صفحهٔ Slide Show را کلیک کنید.

۲. در گروه StartUp، گزینهٔ Record Slide Show را کلیک کنید. گزینهٔ Start Recording From



شکل ۸ـ۱۷ نمایش اسلایدها را ضبط کنید.

Beginning یا Start Recording from Current Slide را کلیک کنید. کادر دیالوگ Record Slide Show باز می‌شود. توجه کنید که اگر میکروفن داشته باشید می‌توانید از گزینهٔ Laser Pointer استفاده کنید (شکل ۸ـ۱۷).

۳. دکمهٔ Start Recording را کلیک کنید. نمایش باز می‌شود.

۴. بگذارید اسلایدها نمایش داده شوند. اگر صدایی ضبط می‌کنید، به گونهٔ روشن در میکروفن صحبت کنید. هنگامی که می‌خواهید به اسلاید بعدی بروید، دکمهٔ Next را از نوار ابزار Recording کلیک کنید. این نوار ابزار در بالا سمت چپ قرار دارد.

۵. هنگامی که به پایان نمایش اسلاید بررسی، پاورپوینت صفحه را می‌بندد. اگر روی اسلایدی صدا ضبط شود، در پایین سمت راست آن یک آیکن بلندگو آشکار می‌شود.

◄ **نکته:** هنگام ضبط، برای اینکه اشاره‌گر ماوس در ضبط نشان داده شود، کلید Ctrl را فشار داده و نگه دارید، سپس دکمهٔ سمت چپ ماوس را فشار دهید. Laser Pointer آشکار می‌شود.

۸ـ۳۷ کار با Animation Pane

Animation Pane امکان نمایش و مدیریت همهٔ افکت‌های اسلاید کنونی را فراهم می‌کند. می‌توانید افکت‌ها را ویرایش و مرتب کنید. هنگامی که شمار افکت‌های اسلاید زیاد است، سودمند است.

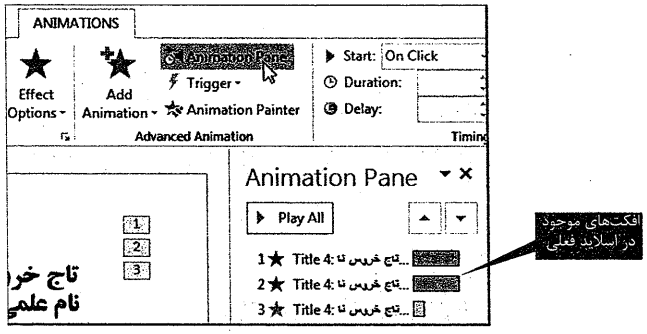
۸ـ۳۷ـ۱ باز کردن Animation Pane

برای باز کردن پنجرهٔ Animation Pane، مرحله‌های زیر را انجام دهید:

۱. در ریبون، در صفحهٔ Animations کلیک کنید.

۲. در گروه Advanced Animation، گزینهٔ Animation Pane را کلیک کنید.

۳. Animation Pane در سمت راست پنجره آشکار می‌شود و همهٔ افکت‌های اسلاید کنونی را نشان می‌دهد.



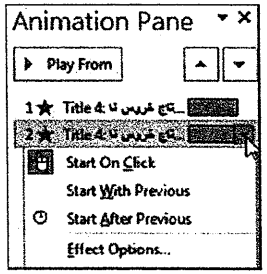
۸ـ۳۷ـ۲ مرتب کردن افکت‌ها در Animation Pane

در پنجرهٔ Animation Pane، یک افکت را کلیک کنید، دکمهٔ ماوس را نگه دارید و آن را به بالا یا پایین ببرید.

۸ـ۳۷ـ۳ نمایش افکت‌ها در Animation Pane

در پنجرهٔ Animation Pane، دکمهٔ Play All را کلیک کنید.

◄ **نکته:** اگر timeline پیدا نبود، فلش بازشوی کنار یک افکت را کلیک کنید و گزینهٔ Show Advanced Timeline را کلیک کنید.



۸ـ۳۷ـ۴ تغییر گزینهٔ آغاز یک افکت

به گونهٔ پیش‌فرض، هنگام پخش اسلاید، با هر کلیک، یک افکت آغاز می‌شود. اگر چند افکت داشته باشید باید چندبار کلیک کنید تا افکت‌ها اجرا شوند. می‌توانید افکت‌ها را به گونهٔ خودکار اجرا کنید. برای این کار، مرحله‌های زیر را انجام دهید:

۱. درAnimation Pane، یک افکت را کلیک کنید.

۲. فلش کنار افکت را کلیک کنید. لیستی باز می‌شود که شامل گزینه‌های زیر است:

- Start on click، سبب می‌شود با کلیک کردن ماوس، افکت اجرا شود.

- Start with previous، سبب می‌شود افکت هم‌زمان با افکت دیگر اجرا شود.
- Start After Previous، سبب می‌شود افکت پس از پایان افکت پیشین اجرا شود.

۳. گزینهٔ آغاز دلخواه را کلیک کنید.

۸ـ۳۸ ایجاد دکمه

افزون بر ابرلینک‌ها از دکمه‌ها نیز برای اتصال به صفحهٔ وب، نشانی رایانامه، یا اسلاید استفاده می‌شود. دکمه‌ها می‌توانند به اسلاید دیگری لینک داشته باشند، صدایی را پخش کنند یا عملی را انجام دهند.

پس از لینک شدن دکمه، اکشنی روی می‌دهد. دکمه‌ها مانند ابرلینک‌ها عمل می‌کنند. می‌توانید از دکمه‌ها برای برگشتن به اسلاید پیشین (برای نمونه صفحهٔ فهرست، یا صفحهٔ عنوان) استفاده کنید. برای ایجاد دکمه مرحله‌های زیر را انجام دهید:

۱. در ریبون، صفحهٔ Insert را کلیک کنید.

۲. گزینهٔ Shape را کلیک کنید، منویی باز می‌شود که دکمه‌ها در انتهای سیاهه (لیست) قرار دارند.

۳. یک دکمه را کلیک کنید. بر روی مکانی از اسلاید کلیک کنید. دکمه در آنجا قرار می‌گیرد. کادر دیالوگ Action Settings باز می‌شود. با انتخاب صفحهٔ Mouse Click، با کلیک کردن دکمه، اکشن آن روی می‌دهد. با انتخاب Mouse Over، هنگامی که اشاره‌گر ماوس روی دکمه قرار گیرد، اکشن آن روی می‌دهد.

۴. در بخش Action on click، فلش سیاهه (لیست) Hyperlink to را کلیک کنید، سپس یکی از گزینه‌های منو را کلیک کنید.

۵. اگر می‌خواهید صدایی پخش شود، کادر کنترل Play Sound را کلیک کنید. سپس فلش سیاهه (لیست) زیر آن را کلیک کنید.

۶. یکی از گزینه‌های این سیاهه (لیست) را کلیک کنید.

۷. OK را کلیک کنید.

۸ـ۳۸ـ۱ ایجاد دکمه روی همهٔ اسلایدها

می‌توانید یک دکمه را بر روی همهٔ اسلایدها ایجاد کنید، برای این کار، مرحله‌های زیر را انجام دهید:

۱. در ریبون، صفحهٔ View را کلیک کنید.

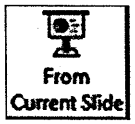
۲. در گروه Master View، گزینهٔ Slide Master را کلیک کنید. یک اسلاید خالی با سبک نمایش شما ایجاد می‌شود.

۳. در ریبون، صفحهٔ Insert را کلیک کنید. با انجام مرحله‌های بخش پیش، یک دکمه ایجاد کنید.

۴. صفحهٔ Slide Master را کلیک کنید و دکمهٔ Close Master View را کلیک کنید.

دکمهٔ جدید بر روی همهٔ اسلایدها به وجود می‌آید.

۸ـ۳۸ـ۲ آزمایش دکمه



پس از ایجاد دکمه، آن را آزمایش کنید. برای این کار، مرحله‌های زیر را انجام دهید:

۱. در ریبون، صفحهٔ Slide Show را کلیک کنید.

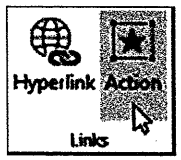
۲. در گروه Start Slide، گزینهٔ From Current Slide را کلیک کنید.

۳. دکمهٔ روی اسلاید را کلیک کنید.

۴. پس از آزمایش دکمه، روی هر چیزی از صفحه کلیک راست کنید و گزینهٔ End Show را کلیک کنید.

۸ـ۳۸ـ۳ ویرایش دکمه

اگر دکمه‌ای به درستی عمل نمی‌کند، آن را ویرایش کنید. برای این کار، مرحله‌های زیر را انجام دهید:



۱. دکمه را برگزینید، سپس در ریبون، صفحهٔ Insert را کلیک کنید.

۲. در گروه Links، دکمهٔ Actions را کلیک کنید.

۳. در کادر دیالوگ Actions Settings، اکشن یا لینک را ویرایش کنید.

۴. OK را کلیک کنید.

۸ـ۳۹ نمایش Slide Master

نمایش Slide Master یک ویژگی در پاورپوینت است که سبب می‌شود اسلایدها و طرح‌کلی اسلایدهای یک نمایش را با سرعت ویرایش کنید. ویرایش Slide Master بر روی هر اسلایدی از نمایش اثر می‌گذارد. می‌توانید برای هر اسلاید یک طرح‌کلی جداگانه ایجاد کنید.

فرض کنید که یک تم پیدا کردید، اما طرح‌کلی اسلایدهای آن تم را نمی‌پسندید. می‌توانید با استفاده از Slide Master طرح‌کلی را آن گونه که می‌خواهید سفارشی‌سازی کنید.

◄ **نکته:** با فعال شدن نمایش Slide Master، صفحهٔ آن روی ریبون آشکار می‌شود.

۸ـ۳۹ـ۱ تغییر دادن همهٔ اسلایدها

اگر می‌خواهید چیزی را از همهٔ اسلایدهای یک نمایش تغییر دهید، برای نمونه به همهٔ اسلایدها یک لوگو بیفزایید، مرحله‌های زیر را انجام دهید:

۱. در ریبون، صفحهٔ View را کلیک کنید. دستور Slide Master را کلیک کنید.

۲. نمایش Slide Master فعال می‌شود و صفحهٔ آن روی ریبون آشکار می‌شود.

۳. از نوار مرور اسلایدها، نخستین اسلاید را برگزینید. این اسلاید، اسلایدِ برتر است.

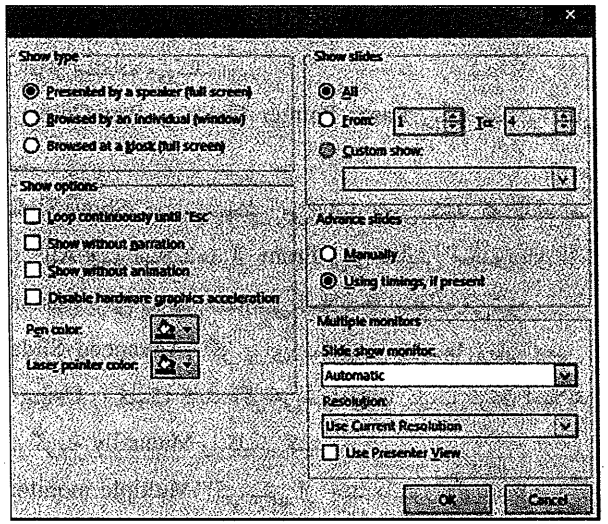
۴. تغییر دلخواه را انجام دهید. برای نمونه، یک تصویر در گوشهٔ سمت چپ اسلاید بیفزایید.

۵. سپس در صفحهٔ Slide Master، گزینهٔ Close Master View را کلیک کنید.

این تغییرها روی همهٔ اسلایدها اعمال می‌شود.

۸ـ۴۰ تعیین نوع ارائهٔ نمایش

پاورپوینت تنظیم‌های متنوعی برای پخش نمایش اسلایدها دارد. برای تعیین نوع ارائهٔ نمایش مرحله‌های زیر را انجام دهید:



شکل ۸ـ۱۸ کادر دیالوگ Set Up Show.

۱.در ریبون، صفحهٔ Slide Show را کلیک کنید. سپس گزینهٔ Set Up Show را کلیک کنید.

۲.کادر دیالوگ Set Up Show باز می‌شود (شکل ۸ـ۱۸).

گزینه‌هایی برای تنظیم و پخش نمایش اسلایدها وجود دارد.

- گزینهٔ Presented by a speaker (full screen)، اسلاید در کل صفحه نمایش داده می‌شود و توسط بلندگو کنترل می‌شود.
- گزینهٔ Browsed by individual (window)، اسلاید در پنجرهٔ پاورپوینت نمایش داده می‌شود.
- گزینهٔ Browsed at the kiosk، اسلاید را در کل صفحه نمایش می‌دهد، اما کنترلی ارائه نمی‌دهد.
- در بخش Show Options این گزینه‌ها وجود دارند:
  - Loop continuously until Esc، اسلایدها تا زمانی که دکمهٔ Esc فشار داده نشود نمایش داده می‌شوند.
  - Show without narration، اسلایدها بدون صدای گوینده پخش می‌شوند.
  - Show without animation، اسلایدها بدون پویانمایی پخش می‌شوند.

- Disable hardware graphics acceleration، برای پخش اسلاید از گرافیک سخت‌افزار استفاده می‌کند.
- گزینهٔ Pen Color و Laser Pointer Color رنگ قلم و اشاره‌گر را تغییر می‌دهند.

- بخش Show Slides، در این بخش می‌توانید معین کنید که کدام اسلایدها نمایش داده شوند. All همهٔ اسلایدها، از From برای نمایش محدوده‌ای از اسلایدها و از Custom Show برای نمایش سفارشی اسلایدها استفاده می‌شود.
- بخش Advanced Slides، اگر برای نمایش اسلایدها زمان معین کردید، گزینهٔ Using Timing را کلیک کنید. اگر می‌خواهید با کلیک کردن اسلاید بعدی نمایش داده شود، گزینهٔ Manually را کلیک کنید.
- بخش Multiple monitors، اگر بیش از چند مانیتور دارید، باید برگزینید که کدام یک اسلاید را نمایش دهد. بهتر است Automatic را انتخاب کنید.

پرسش و پژوهش

۱. چگونگی نمایش اسلایدها را در پاورپوینت بیان کنید.
۲. تصویرها را چگونه به اسلاید می‌افزایید؟
۳. ویدئو را چگونه به اسلاید می‌افزایید؟
۴. صدا را چگونه ضبط و با آن کار می‌کنید؟
۵. چگونه متن و اشیا را به پویانمایی بدل می‌کنید؟
۶. از این فصل از کتاب، یک اسلاید تهیه کنید؟

۹

امنیت اطلاعات

اهداف آموزشی

پس از مطالعهٔ این فصل توانایی‌های زیر را درک خواهید کرد:

با چند تعریف امنیت اطلاعات آشنا می‌شوید.
با اصول سه‌گانهٔ امنیت اطلاعات آشنا می‌شوید.
با گام‌های پیاده‌سازی امنیت اطلاعات آشنا می‌شوید.
با ابعاد مرتبط با امنیت اطلاعات آشنا می‌شوید.
با شماری از راهکارهای عملی بهبود امنیت روی ویندوز ۸ به بعد آشنا می‌شوید (رمزگذاری فایل‌ها، تهیه کپی پشتیبان، کنترل لیست نرم‌افزارهای درحال اجرا).

۹ـ۱ امنیت اطلاعات چیست؟

با توجه به ویژگی‌های عصر امروزی که عصر اطلاعات نیز نامیده شده است مهم‌ترین سرمایه برای هر فرد و یا سازمان اطلاعات است از این رو در این عصر، امنیت اطلاعات جزء یکی از مهم‌ترین مسئله‌های امروزی گشته است.

امنیت اطلاعات به حفاظت از اطلاعات و به کمترین رساندن خطر افشای اطلاعات در بخش‌های غیرمجاز اشاره دارد.

۹ـ۲ آشنایی با اصول امنیت اطلاعات

اندیشیدن امنیت اطلاعات برای دستیابی به سه اصل مهم است که با یکدیگر مثلث امنیتی را تشکیل می‌دهند. این عامل‌ها عبارت‌اند از محرمانگی (Confidentiality)، یکپارچگی و صحت (Integrity) و در نهایت در دسترس بودن همیشگی (Availability) این سه عامل (CIA) اصول اساسی امنیت اطلاعات در شبکه و یا بیرون آن را تشکیل می‌دهند به‌گونه‌ای که همهٔ تمهیدات لازمی که برای امنیت اطلاعات اتخاذ می‌شود و یا تجهیزاتی که ساخته می‌شوند، همگی ناشی از نیاز به اعمال این سه پارامتر در محیط‌های نگهداری و تبادل اطلاعات است.

محرمانگی (Confidentiality)

به معنای آن است که اطلاعات تنها در دسترس کسانی قرار گیرد که به آن نیاز دارند و این‌گونه تعریف شده است. برای نمونه از دست دادن این خصیصه امنیتی معادل است با بیرون رفتن بخشی از پرونده محرمانه یک شرکت و امکان دسترسی به آن توسط مطبوعات.

جامعیت (Integrity)

بیشتر مفهومی است که به علوم سامانه‌ای باز می‌شود و به گونهٔ چکیده می‌توان آن را این‌گونه تعریف کرد:

تغییرها در اطلاعات تنها باید توسط افراد یا فرایندهای مشخص و مجاز انجام گیرد.

تغییرها بدون اجازه و بدون دلیل حتی توسط افراد یا فرایندهای مجاز نباید انجام بگیرد.

یکپارچگی اطلاعات باید در درون و بیرون سامانه حفظ شود. به این معنی که یک داده مشخص چه در درون سامانه و چه در خارج آن باید یکسان باشد و اگر تغییر می‌کند باید هم‌زمان درون و برون سامانه از آن آگاه شوند.

دسترسی‌پذیری (Availibility)

این ویژگی تضمین می‌کند که یک سامانه برای نمونه اطلاعاتی همواره باید در دسترس باشد و بتواند کار خود را انجام دهد؛ بنابراین حتی اگر همه موردهای ایمنی مد نظر باشد، اما عامل‌هایی سبب خوابیدن سامانه شوند ـ مانند قطع برق ـ از نظر یک سامانه امنیتی این سامانه ایمن نیست.

اما جدای از مسئله‌های بالا مفاهیم و پارامترهای دیگری نیز هستند که با وجود آنکه از همین اصول گرفته می‌شوند برای خود شخصیت جداگانه‌ای پیدا کرده‌اند. در این میان می‌توان به مفاهیمی مانند Authentication به معنی احراز هویت کاربر، Authorization به معنی مشخص کردن میزان دسترسی کاربر به منابع، Accountability به معنی قابلیت حسابرسی و ثبت لاگ از عملکرد سامانه و کاربران سامانه و ... اشاره کرد.

۹ـ۳ پیاده‌سازی امنیت اطلاعات

برای برقراری مدیریت امنیت اطلاعات شش گام به شرح زیر متصور است:

▪ **گام۱:** توسعه، تصویب و ترویج خط‌مشی امنیت اطلاعات فراگیر:

باید با نظر کارشناسان خبره بخش‌های گوناگون دنباله‌ای از خط‌مشی‌های امنیت اطلاعات را مبنی بر استاندارد موجود توسعه، تصویب واجرا کرد. این دستور کار به صورت رسمی برنامهٔ امنیت اطلاعات سازمان را بیان می‌کند و کارکنان در برابر آن پاسخگو هستند. فهرست زیر شامل مجموعه‌ای از خط‌مشی‌ها رسمی سازمانی را بیان می‌کند و البته فقط محدود به موارد زیر نمی‌شود:

ـ به‌روزرسانی و اجرا کردن خط‌مشی پذیرفتنی در کاربرد رایانه و شبکه به صورت عمومی؛

ـ کنترل دسترسی اطلاعات و تعیین سطح دسترسی به داده‌ها و سامانه‌ها؛

ـ اعلام وصول، ذخیره‌سازی و پردازش و پخش اطلاعات حساس؛

ـ آزمایش و بازبینی امنیتی سخت‌افزار و نرم‌افزار به‌کار گرفته‌شده؛

ـ ممارست در حفاظت از داده‌های عمومی به صورت گزارش‌گیری از تخلف‌ها و تهدیدهای امنیتی؛

ـ مجوزهای قانونی تخریب، پشتیبان‌گیری و وضعیت رسانه‌های دیجیتالی؛

ـ حذف دسترسی‌های کارکنان که فعالیتشان به هر دلیلی پایان یافته است.

ـ ارزیابی و مدیریت مخاطره‌ها (ریسک).

▪ **گام۲:** کارکنان باید آگاه از پاسخگویی دربارهٔ امنیت اطلاعات باشند:

همه کارکنان باید در دورهٔ آشنایی و یادگیری امنیت اطلاعات و به‌کار بردن اصول حفاظت از اطلاعات سازمان شرکت کنند. برنامهٔ آموزشی باید دارای سطح‌بندی انعطاف‌پذیری برای مدیران ارشد، مدیران میانی، مدیران سامانه و شبکه و کارکنان

بخش‌های گوناگون باشد. برنامهٔ آموزشی با توجه به نوع فعالیت هر فرد و پاسخگو بودن در برابر سازمان تنظیم شود. مرحله‌های ساخت برنامه آموزشی شامل معیارهای زیر است:

- شناسایی و تحلیل فاصله میان وضعیت جاری و دانش مطلوب؛
- تعیین اولویت‌ها؛
- توسعهٔ آگاهی (با پست الکترونیک و صفحه‌های وب و خبرنامه‌ها)؛
- انتخاب موضوع‌های آموزشی (خط‌مشی‌های قابل اجرا)؛
- توسعهٔ آموزش و یادگیری براساس وظیفه و مسئولیت؛
- استفاده از فناوری برای آموزش (کاربرد وب، آموزش الکترونیک).

▪ **گام ۳:** ایجاد امور امنیت اطلاعات هر بخش:

در هر بخش فردی که توانایی مناسبی برای پیاده‌سازی و اجرای خط‌مشی‌های مورد نیاز امنیت اطلاعات دارد انتخاب شود. واحد امنیت اطلاعات در موارد زیر پاسخگو است والبته فقط محدود به موارد زیر نمی‌شود:

- توسعه، انتشار، نگهداری رویه‌ها، خط‌مشی‌های برنامهٔ امنیت سامانه‌های اطلاعاتی در بخش مربوطه؛
- متصدی رسیدگی به اعتراض‌ها، شکایت‌ها و تخلف‌های حوزهٔ تبادل اطلاعات و اهتمام در به نتیجه رساندن آنها؛
- متصدی کنترل نقاط اصلی در هنگام وقوع رویدادهای امنیتی و وخیم؛
- فراهم کردن پیشنهادهایی برای مدیران راهبردی (استراتژیک) که نیازمندی‌های مدیریت مخاطره‌ها و بحث‌های مربوط به فناوری سامانه‌های اطلاعاتی را پوشش دهد.

متصدی واحد امنیت اطلاعات بخش باید فعالیت‌های غیررسمی پیرامون امنیت اطلاعات نیز داشته باشد. موارد زیر پاسخگویی‌های غیررسمی متصدی واحد امنیت اطلاعات است والبته فقط محدود به این موارد نمی‌شود:

- مطمئن ساختن کارکنان به مناسب بودن نسبی خط‌مشی و دستور کارهای امنیت اطلاعات؛
- مطمئن شدن از انطباق امنیت پیاده‌شده بر راهبرها و خط‌مشی‌های امنیتی؛
- گزارش دادن به مدیر امنیت اطلاعات مبنی بر سنجش و ارزیابی قوانین مصوب مسئولان اجرایی.

▪ **گام ۴:** بنا نهادن فرایندی برای گزارش‌گیری منظم از پیشرفت کارها و ارائهٔ آن به مدیر اجرایی:

دفتر پیاده‌سازی امنیت باید دارای زمان‌بندی مشخصی برای گزارش پیشرفت و توسعه امنیت اطلاعات به رئیس سازمان داشته باشد. این گزارش‌ها در دو بعد قابل استفاده است:

۱) ارزیابی مسئول سازمان از توانمندی پیاده‌سازی امنیت اطلاعات توسط تیم اجرایی؛

۲) برطرف کردن نقص‌ها و ایرادهای خط‌مشی‌های امنیتی تصویب‌شده توسط مسئولان کلان سازمان.

▪ **گام ۵:** پیاده کردن کنترل‌های فعال وگسترده:

تعیین سامانه‌هایی که دارای اطلاعات حساس هستند و مطمئن بودن از استقرار کنترل‌های دسترسی و سامانه‌های اطلاعاتی که هر شخص فقط به اطلاعات مشخصی دسترسی دارد انواع کنترل دسترسی شامل کنترل دسترسی اجباری، احتیاطی، مبنی بر مسئولیت سازمانی و زمانی از روز است. اهم نظارت‌ها در این بخش عبارت‌اند از:

- ارزیابی بخش‌ها در راه‌اندازی خط‌مشی امنیتی؛
- شناسنامه‌دار کردن دستگاه‌ها؛
- تاکید بر پیچیدگی رمز عبور؛
- تاکید بر تغییر رمز به صورت دوره‌ای؛
- ثبت عملکرد کاربران در سامانه‌های اطلاعاتی.

▪ **گام ۶:** پیاده کردن و ارتقای پیوسته و برنامه‌های ترسیم رویدادها:

سازمان باید به صورت پیوسته به تحلیل و ارزیابی مخاطره‌های سازمانی بپردازد و برنامهٔ مشخص بخشی و سازمانی برای حفاظت و ترمیم سامانه‌های حساس، سرویس‌های شبکه و برنامه‌های کاربردی و داده‌ها داشته باشد. برنامه ارتقای مداوم عبارت است از:

- کنترل وارزیابی مخاطره‌ها؛
- تحلیل آسیب‌های حرفه و کسب و کار؛
- توسعهٔ مداوم راهبرد (استراتژی)های حرفه؛

ـ طراحی دفتر واکنش و فرایند؛
ـ آگاهی، آموزش و یادگیری؛
ـ معاونت و نگهداری پیوسته از برنامه‌های سازمانی.

۹ـ۴ ابعاد مرتبط با امنیت

ابعاد مرتبط با امنیت شامل سه بُعد است:
ـ امنیت فیزیکی
ـ امنیت عملیاتی
ـ مدیریت و تدابیر امنیتی

۱. برقراری امنیت فیزیکی (Physcial Security)

منظور از امنیت فیزیکی، حفاظت از دارایی‌ها و اطلاعات در برابر دسترسی فیزیکی افراد یا کارکنان غیرمجاز است. به عبارت دیگر شما مسئول حفاظت از بخش‌هایی هستید که قابل لمس کردن، دیده شدن و دزدیده شدن هستند. این تهدیدها بیشتر توسط سرویس‌کارها، دربان‌ها یا سرایدارها، مشتری‌ها، فروشنده‌ها و حتی کارمندان به‌وجود می‌آیند.

این‌گونه افراد می‌توانند ابزارها را ببینند و یا آنها را خراب کنند، یا از دفتر کار مدارک و اسنادی را به سرقت ببرند و یا در درون آنها اطلاعات ناخواسته قرار دهند، انگیزهٔ آنها در انجام این کارها می‌تواند انتقام گرفتن از شما باشد، حال این انتقام می‌تواند به خاطر به‌وجود آمدن یک سوء تفاهم باشد و یا اینکه به خاطر کینه‌جویی آن فرد نسبت به شما باشد و به همین دلیل، اطلاعات محرمانه شما را به سرقت برده و در اختیار رقیبان شما قرار می‌دهند.

پیاده‌سازی امنیت فیزیکی به نسبت کار آسانی است، شما می‌توانید تأسیسات خود را با استفاده از کنترل کردن دسترسی به دفتر کارتان ایمن کنید، مدارک و اسناد غیرضروری را ریز ریز کنید (نوعی حمله به نام dumpster diving معروف است) سامانه‌های امنیتی نصب کنید و به بخش‌های ویژه‌ای از فعالیت‌های بازرگانی خود محدودیت دسترسی بدهید.

بیشتر سازمان‌های اداری در ساعت‌های غیرفعال کاری محیط اطراف ساختمان را

تحت پوشش امنیتی قرار می‌دهند و به این وسیله آنجا را ایمن می‌کنند، همین کار را می‌توان در ساعت‌های اداری و فعال سازمان‌ها نیز اعمال کرد و چندان هم که به نظر می‌رسد دشوار نیست. بسیاری از سازمان‌ها و شرکت‌ها از سامانه‌های گوناگون امنیتی مانند نگهبان، قفل‌های کنترل ورود و خروج، سامانه‌های الکترونیک رمز ورود، دوربین‌های امنیتی، درگاه‌های کنترل و بازرسی بدنی و بسیاری دیگر از امکانات و تجهیزات امنیتی استفاده می‌کنند. در بیشتر موارد مدیران بخش‌ها به امنیت درونی بخش‌ها که مربوط به رایانه‌ها، اسناد و مدارک شخصی شما است سروکاری ندارند، در واقع حفاظت از این موارد جزء وظایف شخصی شما در آن بخش است.

نخستین جزء امنیت فیزیکی این است که شما وسوسه‌انگیزی سامانهٔ خود را تا حد امکان کم کنید، یعنی اینکه تا جایی که امکان دارد کاری کنید که محیط واقعی کمتر در معرض دید باشد. فرض کنید شما یک فروشگاه جواهرآلات دارید، این طبیعی است که در هنگامی که شما در تعطیلات بسر می‌برید ویترین فروشگاه خود را جمع کرده و آنها را در درون گاوصندوق قرار می‌دهید. دزدان با دیدن جواهر انگیزه بیشتری برای دزدی پیدا می‌کنند، اگر آنها را نبینند و در معرض دید نباشند انگیزه دزدان نیز به مراتب کمتر خواهد شد. این کاملاً طبیعی است که اگر کسی بتواند سرورهای شما را ببیند بیشتر از شخصی که آنها را نمی‌بیند وسوسه نفوذ به آنها را پیدا می‌کند. اگر شرکت یا سازمان شما به صورت تمام وقت باز است دسترسی به منابع تجاری موجود در آن نیز به مراتب آسان‌تر است، شما باید تا حد امکان سازمان خود را از معرض دید دیگران دور نگه دارید. قفل کردن درها، نصب سامانه‌های دیدبانی و نظارتی و نصب انواع هشداردهنده‌ها می‌تواند محیط فیزیکی را تا حد زیادی ایمن کند. در پیش هم به این موضوع اشاره شد که همیشه در این تفکر باشید که در حال هک شدن هستید، بنابراین کوشش کنید با ساده‌ترین فرایندهای ممکن امنیت را بالا برده تا با دشواری‌های ساده به دردسر نیفتید.

دومین بخش امنیت فیزیکی دربرگیرندهٔ تشخیص نفوذ یا دزدی است، شما باید بدانید چه کسی یا چه چیزی وارد شده است و یا از میان رفته است. باید بدانید که چه چیزهایی ناپدید شده است و این تغییرها چگونه روی داده است. دوربین‌های مدار بسته روش بسیار خوبی برای به دست آوردن این اطلاعات است. بیشتر شرکت‌های کوچک برای تشخیص چگونگی رخ دادن دزدی‌ها و اینکه چه کسی آن را انجام داده است از

این گونه دوربین‌ها استفاده می‌کنند. فیلم‌هایی که از این گونه دوربین‌ها به دست می‌آید در بیشتر دادگاه‌ها مدارک و اسناد قابل استنادی به‌شمار می‌آیند. به عنوان یک مدیر شبکه شرکت، شما باید بی‌درنگ پس از رخ دادن دزدی، به هیچ چیز دست نزنید، و با سرعت موضوع را به مراجع قانونی اطلاع دهید تا به بررسی موضوع بپردازند. این نکته را به یاد داشته باشید که در چنین حالتی شما باید به هر کسی که فکر می‌کنید ظنین باشد.

سومین بخش امنیت فیزیکی ارزیابی اطلاعات ازدست‌رفته است. فرض کنید که اطلاعات حیاتی یک شرکت از میان رفته است، چه‌کار باید کرد؟ چگونه یک سازمان پس از به‌وقوع پیوستن یک دزدی یا فاجعه می‌تواند به حالت عادی خود بازگردد؟ با یک نمونه این موضوع روشن‌تر می‌شود، فرض کنید یک خرابکار اتاق سرورهای شما را که همهٔ اطلاعات حیاتی سازمان شما در آن وجود دارد را به آتش می‌کشد و یا در استان گلستان هستید و سیل به‌وجود آمده همهٔ اداره شما را می‌شوید و از میان می‌برد، یا در تهران هستید و زلزله‌ای رخ داده و دفتر کار شرکت به صورت کامل از میان می‌رود، البته فرض را در این می‌گیریم که در همهٔ شرایط بالا شما در امنیت کامل بسر می‌برید و پس از فاجعه فرصت رسیدگی به موضوع را دارید. یا ساده‌ترین نمونه اینکه در هنگام کار کردن با سرورها در اتاق سرور یک پارچ آب به صورت کامل روی سرورها ریخته و همهٔ اطلاعات سرور از میان می‌رود! چقدر طول می‌کشد تا سازمان فعالیت عادی خود را که به اطلاعات یادشده وابسته است را از سر گیرد؟

۲. برقراری امنیت عملیاتی(Operational Security)

امنیت عملیاتی یا اجرایی شیوهٔ انجام دادن کارهای سازمان را بیان می‌کند. در معنای عام می‌توان به عنوان مدیریت اطلاعات از آن نام برد. امنیت عملیاتی پهنه وسیعی را دربر می‌گیرد که شما هم بخشی از آن هستید. اصول امنیت عملیاتی شامل: کنترل دسترسی، شناسایی و مکان‌شناسی (توپولوژی‌های) امنیتی است. موارد یادشده شامل فعالیت‌های روزانه شبکه، اتصال به شبکه‌های دیگر، طراحی شیوهٔ تهیه نسخهٔ پشتیبان و طراحی شیوهٔ بازگردانی آن می‌شود که البته همهٔ این موارد در حالتی امکان‌پذیرند که نصب شبکه کامل شده باشد. اگر بخواهیم امنیت عملیاتی را در یک جمله خلاصه کنیم به این صورت بیان می‌شود: شامل هر چیزی در شبکه شما می‌شود که به طراحی و امنیت فیزیکی شما بستگی ندارد.

در این بخش به جای اینکه تمرکز خود را بر تجهیزات فیزیکی قرار دهیم، بیشتر به مکان‌شناسی (توپولوژی)ها و اتصال‌ها و پیکربندی‌ها توجه می‌کنیم. فرایندی که شما باید در بخش فیزیکی انجام دهید در ابتدا بسیار طاقت‌فرسا به نظر می‌رسد. در بسیاری اوقات شما از نقاط آسیب‌پذیر شبکه بدون اینکه بدانید در حال استفاده هستید و یا بدون اطلاع، خط‌مشی را پیاده‌سازی کرده‌اید که دارای ضعف امنیتی است یا ناقص است. برای نمونه شما خط‌مشی را پیاده‌سازی کرده‌اید که در آن کاربران مجبور هستند که رمزهای گذر خود را هر ۳۰ یا ۶۰ روز عوض کنند، حال اگر در سامانهٔ شما قابلیت استفاده از سامانهٔ چرخش رمز گذر طراحی نشده باشد (این سامانه به شما اجازهٔ استفاده از رمزهای گذر تکراری مورد استفاده در زمان‌های گذشته را نمی‌دهد) شما یک نقطهٔ آسیب‌پذیر جدی در شبکهٔ خود دارید که شاید نتوانید آن را از میان ببرید، در این حالت از نظر دیدگاه فرایندی سامانه قابلیت رمز گذر ضعیفی دارد. در این حالت شما دو گزینه برای انتخاب دارید، یا باید فرایند امنیتی اطلاعات را به‌گونهٔ کامل ارتقا دهید و یا اینکه سیستم عامل را به‌گونهٔ کلی عوض کنید. انجام دادن هریک از این فرایندها دشواری‌های ویژه خود را مانند میزان بودجه، زمان بدل و بی‌میلی سازمان برای انجام این کار را دربر دارد. گفتنی است که متأسفانه یا خوشبختانه در کشور عزیز ما ایران به علت نبود قانون کپی رایت، دشواری تعویض سیستم عامل وجود ندارد زیرا هزینه‌ای برای تعویض آن و تهیه سیستم عامل نو پرداخت نمی‌شود، اما فرض را بر این بگیرید که در شرکتی هستید که به‌گونهٔ متوسط ۲۰۰ عدد سیستم عامل ویندوز ایکس پی در آن مشغول کار هستند، حال اگر باید ۲۰۰ عدد سیستم عامل، دست‌کم ۶۰ دلاری، خریداری شود هزینه‌ها بسیار بالا می‌رود، ذهن خود را درگیر CDهایی نکنید که در بازار یا کنار خیابان فروخته می‌شوند و ۸ سیستم عامل روز جهان را با بهای کمتر از هزار تومان به مردم عرضه می‌کنند.

اما دشواری اصلی، بی‌میلی سازمان و مدیران برای انجام تغییرها در سازمان است. متأسفانه برخی از مدیران سنتی عمل می‌کنند و از انجام دادن تغییرها در روند ایجاد محیطی ایمن می‌هراسند، یا احساس بی‌میلی دارند که از نظر بسیاری از کارشناسان بزرگ‌ترین دشواری موجود در برقراری امنیت عملیاتی همین مورد است، اگر مدیر نخواهد کاری انجام شود، پس نمی‌شود تلاش بیهوده نکنید. اما هر دشواری راهکاری نیز دارد که به آن خواهیم پرداخت.

اگر سیستم عامل شما داری نقاط ضعف امنیتی زیادی باشد متقابلاً وظیفه شما نیز افزایش می‌یابد زیرا همچنان شما مسئول برقراری امنیت در آنجا هستید، برای نمونه: اگر شبکه شما که تا حدی ایمن است به اینترنت متصل شود، هدف نفوذ بسیاری از افراد قرار خواهد گرفت، حال شما می‌توانید با نصب نرم‌افزارها و سخت‌افزارهای امنیتی، امنیت را تا حد مطلوبی افزایش دهید. در هر حال مدیران باور دارند که این گونه ابزارها برای پیاده‌سازی پرهزینه هستند، بنابراین شما کار زیادی نمی‌توانید انجام دهید. تنها راه‌حلِ قانع کردن مدیران، نشان دادن شدت تهدیدهایی است که ممکن است عملکرد شرکت یا سازمان را مختل کند و آن را گرفتار تهدید کند. در زیر می‌توانید چکیده مواد مرتبط با امنیت عملیاتی را ببینید:

رایانه	شبکه	خط‌مشی‌ها
مدیریت	کنترل دسترسی	شناسایی
طرح و نقشه تهیه نسخه پشتیبان و بازگردانی آن		

۳. مدیریت و خط‌مشی‌ها (Management and Policies)

مدیریت و خط‌مشی‌ها در واقع برنامه‌هایی هستند که با توجه به آنها می‌توانیم امنیت یک محیط را پیاده‌سازی کنیم. خط‌مشی‌ها برای اینکه کارا باشند نیاز به پشتیبانی همه جانبه از جانب تیم مدیریتی سازمان دارند. راهنماهای درست نه تنها می‌توانند سبب به‌وجود آمدن ابتکارهای امنیتی در محیط شوند بلکه سبب به‌وجود آمدن یک امنیت کارا نیز هستند. متخصصان امنیت اطلاعات می‌توانند خط‌مشی‌های امنیتی خود را ادامه دهند، اما برای اینکه بتوانند آنها را پیاده‌سازی کنند نیاز به پشتیبانی مدیران دارند، این نکته را همیشه به یاد داشته باشید که شما هیچ وقت نمی‌توانید ادعا کنید که شبکه من ایمن است و این در حالی باشد که از پشتیبانی مدیران برخوردار نیستید.

تصمیم‌هایی که باید در سطح مدیریت و خط‌مشی‌ها اتخاذ شود به گونهٔ کامل سازمان را زیر پوشش قرار می‌دهد و می‌تواند بهره‌وری، روحیه کاری و فرهنگ سازمان را تحت تأثیر خود قرار بدهد. این گونه تصمیم‌ها و خط‌مشی‌ها می‌تواند تأثیر بسزایی بر روی مسئله‌های مرتبط با امنیت نیز داشته باشد. این گونه خط‌مشی‌ها باید به‌گونه‌ای طراحی شوند که هدایت سازمان، آسانی در مواقعی که سازمان در تعطیلات به‌سر می‌برد یا کارمندان به مرخصی می‌روند و یا کار آنان به پایان می‌رسد را به گونهٔ کامل زیر پوشش قرار دهند.

بیشتر افرادی که در یک سازمان فعالیت می‌کنند می‌توانند به‌آسانی به شما بگویند که چه مدت زمانی را در طی سال در مرخصی به‌سر می‌برند و همچنین بسیاری دیگر به شما می‌توانند اطلاعات دقیقی از چگونگی استفاده اطلاعات در سازمان و اینکه خط‌مشی‌ها چگونه پیاده‌سازی شده‌اند را در اختیارتان قرار دهند، پس همیشه کاربران و کارمندان را می‌توانید در نقش یک منبع اطلاعاتی بسیار کارا در پیاده‌سازی فعالیت‌های امنیت خود در نظر بگیرید.

برای برقراری امنیت در یک شبکه چندین خط‌مشی کلیدی وجود دارد، سیاهه (لیست) زیر نشان‌دهندهٔ شماری از این خط‌مشی‌های گسترده است که هر کدام نیاز به طراحی و تفکر دارند:

خط‌مشی‌های مدیریتی (Management Policies)

نیازهای طراحی نرم‌افزار (Software Design Needs)

طرح و برنامهٔ بازیابی از حادثه (Disaster Recovery Plan)

خط‌مشی‌های اطلاعاتی (Information Policies)

خط‌مشی‌های امنیتی (Security Policies)

خط‌مشی‌های مدیریتی کاربران (User Management Polices)

۹ـ۵ تدابیر و فرایند لازم برای امنیت فناوری اطلاعات

اگر می‌خواهیم علاوه بر مصرف‌کنندهٔ اطلاعات، ارائه‌دهندهٔ اطلاعات در عصر اطلاعات باشیم، باید در مراحل بعد، امکان استفاده از اطلاعات ذیربط را برای متقاضیان محلی و جهانی در باسرعت‌ترین زمان ممکن فراهم کنیم.

سرعت در تولید و عرضهٔ اطلاعات ارزشمند، یکی از رموز موفقیت در سازمان‌ها، مؤسسه‌ها و جوامع علمی در عصر اطلاعات است. پس از سازماندهی اطلاعات باید با بهره‌گیری از شبکه‌های رایانه‌ای، زمینه استفاده قانونمند و هدفمند از اطلاعات را برای دیگران فراهم کرد. به موازات حرکت به سمت یک سازمان پیشرفته و مبتنی بر فناوری اطلاعات، باید تدابیر لازم برای حفاظت از اطلاعات نیز اندیشیده شود.

مهم‌ترین برتری و رسالت شبکه‌های رایانه‌ای، اشتراک منابع سخت‌افزاری و نرم‌افزاری و دستیابی با سرعت و آسان به اطلاعات است. کنترل دستیابی و شیوهٔ