راهنمای
امنیت فناوری اطلاعات

تألیف:

جورج سادوسکای

جیمز اکس. دمپزی

آلن گرین‌برگ

باربارا جی. مک

آلن شوارتز

ترجمه:

مهدی میردامادی

زهرا شجاعی

محمدجواد صمدی

دبیرخانه

شورای‌عالی اطلاع‌رسانی

تیرماه ۱۳۸۴

راهنمای امنیت فناوری اطلاعات = IT Security Handbook / نویسندگان جورج سادوسکای ... [و دیگران]؛ گروه مترجمین مهدی میردامادی، زهرا شجاعی، محمدجواد صمدی. -- تهران، شورای عالی اطلاع‌رسانی، دبیرخانه، ۱۳۸۴.

۵۰۹ ص.:جدول. ۵۰،۰۰۰ ریال

ISBN: 964-8846-26-x

عنوان به انگلیسی:
IT Security Handbook

فهرستنویسی بر اساس اطلاعات فیپا.

کتابنامه: ص. ۵۰۹ همچنین به صورت زیرنویس. نمایه.

۱. تکنولوژی اطلاعات -- اقدامات تأمینی. الف. سادوسکای، جورج، George، Sadowsky. ب.میردامادی، مهدی - ۱۳۵۹ - -، مترجم. ج.شجاعی، زهرا، مترجم. د.صمدی، محمدجواد، مترجم. هـ .شورای عالی اطلاع‌رسانی. دبیرخانه. و.عنوان.

T۵۸/۵/ر۲۳ ۱۳۸۴ ۳۰۳/۴۸۳۳

کتابخانه ملی ایران ۸۴م-۱۷۵۲۵

این کتاب ترجمه‌ای است از:

George Sadowsky; James X. Dempsey; Alan Greenberg; Barbara J. Mack; Alan Schwartz; *IT Security Handbook*; infoDev, Worldbank; 2003.

(ISBN: 964-03-9951-5; *http://www.infodev-security.net/handbook*)

راهنمای امنیت فناوری اطلاعات

مؤلفین: جورج سادوسکای، جیمز اکس. دمپزی، آلن گرین‌برگ، باربارا جی. مک، آلن شوارتز

گروه مترجمین: مهدی میردامادی (mirmahdi@ashnasecure.com)

زهرا شجاعی (z.shojaee@ashnasecure.com)

محمدجواد صمدی (m.samadi@ashnasecure.com)

ویرایش فنی: مهدی میردامادی

صفحه‌آرایی و نسخه‌پردازی: ماریا قادری (maria_ghaderi@yahoo.com)

لیتوگرافی، چاپ و صحافی: شرکت انتشارات گل‌واژه

ناظر چاپ: سعید زراعتی (ss_zeraati@yahoo.com)

نوبت چاپ: اول ۱۳۸۴

شمارگان: ۱۵۰۰ نسخه

شابک: ISBN: 964-8846-26-x / ۹۶۴-۸۸۴۶-۲۶-x

شمارهٔ پیاپی انتشارات دبیرخانه: ۱۴-۸۴

قیمت: ۵۰،۰۰۰ ریال

نشانی پستی: تهران، خیابان شریعتی، نرسیده به چهارراه شهید قدوسی، نبش اندیشه یکم، شمارهٔ ۸۰۸

تلفن: ۸۸۴۴۸۰۳۷ و ۸۸۴۴۸۰۳۸ **نمابر:** ۸۸۴۴۸۰۳۸ ، ص.پ: ۱۳۱۵ـ ۱۶۳۱۵

نشانی وبگاه: http://www.scict.ir

فهرست

پیش‌گفتار

مفهوم امنیت در دنیای واقعی مفهومی حیاتی و کاملاً شناخته‌شده برای بشر بوده و هست. در دوران ماقبل تاریخ، امنیت مفهومی کاملاً فیزیکی را شامل می‌شد که عبارت بود از اصول حفظ بقا نظیر امنیت در برابر حملهٔ دیگران یا حیوانات و نیز امنیت تأمین غذا. بتدریج نیازهای دیگری چون امنیت در برابر حوادث طبیعی یا بیماریها و در اختیار داشتن مکانی برای زندگی و استراحت بدون مواجهه با خطر به نیازهای پیشین بشر افزوده شد. با پیشرفت تمدن و شکل‌گیری جوامع، محدودهٔ امنیت ابعاد بسیار گسترده‌تری یافت و با تفکیک حوزهٔ اموال و حقوق شخصی افراد از یکدیگر و از اموال عمومی، و همچنین تعریف قلمروهای ملی و بین‌المللی، بتدریج مفاهیم وسیعی مانند حریم خصوصی، امنیت اجتماعی، امنیت مالی، امنیت سیاسی، امنیت ملی و امنیت اقتصادی را نیز شامل گردید. این مفاهیم گرچه دیگر کاملاً محدود به نیازهای فیزیکی بشر نمی‌شدند، ولی عمدتاً تحقق و دستیابی به آنها مستلزم وجود و یا استفاده از محیط‌های واقعی و فیزیکی بود.

لیکن جهان در دهه‌های اخیر و بویژه در پنج سال گذشته عرصهٔ تحولات چشمگیری بوده که بسیاری از مناسبات و معادلات پیشین را بطور اساسی دستخوش تغییر نموده است. این تحولات که با محوریت کاربری وسیع از فناوری اطلاعات و ارتباطات امکانپذیر شده، از کاربرد رایانه به عنوان ابزار خودکارسازی (Automation) و افزایش بهره‌وری آغاز گردیده و اکنون با تکامل کاربری آن در ایجاد فضای هم‌افزائی مشارکتی (Collaboration)، عملاً زندگی فردی و اجتماعی بشر را دگرگون ساخته است. به باور بسیاری از صاحبنظران همانگونه که پیدایش خط و کتابت آنچنان تأثیر شگرفی بر سرنوشت انسان برجای گذاشته که مورخین را برآن داشته تا داستان زندگی بشر بر این کره خاکی را به دوران ما قبل تاریخ و تاریخ تقسیم نمایند، ورود به فضای مجازی حاصل از فناوری نوین اطلاعات و ارتباطات نیز دورهٔ جدیدی از تمدن بشری را رقم زده، بنحوی که انقلاب عصر اطلاعات شیوهٔ اندیشه، تولید، مصرف، تجارت، مدیریت، ارتباط، جنگ و حتی دینداری و عشق‌ورزی را دگرگون ساخته است.

این تحول بزرگ الزامات و تبعات فراوانی را به همراه داشته که از مهمترین آنها بوجود آمدن مفاهیم نوین امنیت مجازی یا امنیت در فضای سایبر می‌باشد. با تغییری که در اطلاق عبارت "شبکهٔ رایانه‌ای" از یک شبکهٔ کوچک کارگروهی به شبکه‌ای گسترده و جهانی (اینترنت) واقع گردیده، و با توجه به رشد روزافزون تعاملات و تبادلاتی که روی شبکه‌های رایانه‌ای صورت می‌پذیرد، نیاز به نظام‌های حفاظت و امنیت الکترونیکی جهت ضمانت مبادلات و ایجاد تعهد قانونی برای طرفهای دخیل در مبادله بسیار حیاتی است. نظام‌هایی مشتمل بر قوانین، روشها، استانداردها و ابزارهایی که حتی از عقود متداول و روشهای سنتی تعهدآورتر بوده و ضمناً امنیت و خصوصی بودن اطلاعات حساس مبادله‌شده را بیش از پیش تضمین نمایند.

امنیت اطلاعات در محیط‌های مجازی همواره بعنوان یکی از زیرساختها و الزامات اساسی در کاربری توسعه‌ای و فراگیر از ICT مورد تاکید قرار گرفته است. گرچه امنیت مطلق چه در محیط واقعی و چه در فضای مجازی دست‌نیافتنی است، ولی ایجاد سطحی از امنیت که به اندازهٔ کافی و متناسب با نیازها و سرمایه‌گذاری انجام شده باشد تقریباً در تمامی شرایط محیطی امکانپذیر است. تنها با فراهم بودن چنین سطح مطلوبی است که اشخاص حقیقی، سازمانها، شرکتهای خصوصی و ارگانهای دولتی ضمن اعتماد و اطمینان به طرفهای گوناگونی که همگی در یک تبادل الکترونیکی دخیل هستند و احتمالاً هیچگاه یکدیگر را ندیده و نمی‌شناسند، نقش مورد انتظار خود بعنوان گره‌ای مؤثر از این شبکه متعامل و هم‌افزا را ایفا خواهند نمود.

اطمینان از ایمن بودن سرمایه های اطلاعاتی و تجهیزات زیرساختی کشور گذشته از ابعاد گسترده امنیت ملی، کلید قفل فرصتهای بی‌شمار تجاری و غیرتجاری جدید اینترنتی است. آنچه مسلم است چالش امنیتی رودرروی کشور عدم دسترسی به فناوری و یا عدم وجود محصولات امنیتی نیست، بلکه سیاستگذاری، فرهنگ‌سازی، بهره‌وری مناسب از منابع موجود و نیز سازگاری آنها به گونه‌ای است که نیاز منحصربه‌فرد شبکه و فضای دیجیتالی کشور را تأمین کند. در این راستا توجه به این نکته ضروری

است که معماری امنیت اطلاعات فرآیندی از فرآیندهای جاری در معماری فناوری اطلاعات در سطوح مختلف اعم از ملی و سازمانی است که در این فرآیند به تناسب و نیاز از ابزارهای لازم استفاده خواهد شد. نکتهٔ مهم دیگر حاصل از تجارب کشورهای پیشرو حاکی است که امنیت اطلاعات مسألهای فرابخشی است و نیاز به همکاریهای گسترده در این زمینه دارد. این همکاریها هم در سطح ملی و هم در سطح بین‌المللی باید مورد توجه قرار گیرد. تعیین نقشها، وظایف و مسئولیتها از نکات مهمی است که در این همکاریها باید تعریف شوند.

امروزه امنیت فضای دیجیتال وجه تازه‌ای از امنیت ملی هر کشور را به تصویر می‌کشد. امید است که به موازات توسعه سریع کاربری‌های گوناگون فناوری ارتباطات و اطلاعات در زیربخشهای مختلف در پوشش برنامهٔ تکفا، با شناخت و تعیین زیرساختهای کلیدی کشور که وابستگی حیاتی به اطلاعات دارند و سپس برنامه‌ریزی، سازماندهی و سرمایه‌گذاری مناسب جهت حفاظت از این زیرساختها، مسیر توسعهٔ همه‌جانبهٔ کشور در دستیابی به جامعهٔ دانایی‌محور هموار گردد.

خوشبختانه در طی سالهای اخیر و پس از تصویب برنامهٔ توسعهٔ و کاربری فناوری اطلاعات و ارتباطات (تکفا) در هیأت دولت که نشان از توجه و بینش مدیریت ارشد کشور در رویکرد نوین به توسعه کشور داشته، مطالعات و بررسیهای فنی برای تمهید نیازهای امنیتی و امنیت در محیطهای رایانه‌ای آغاز شده و رشد سریعی یافته است. نتایج مطالعات کارگروه مرتبط، منجر به شناخت زمینه‌های وسیعتر نیاز گردید و بر این اساس با تصویب هیأت محترم دولت و رئیس محترم جمهور، شورای‌عالی امنیت محیط رایانه‌ای و اینترنتی کشور با مسئولیت معاون اول محترم رئیس جمهور آغاز به کار کرده است و انشاالله بزودی نتایج بررسیها و تصمیمات در قالب دستورالعملها و سند ملی امنیت فضای رایانه‌ای کشور اعلام می‌گردد.

دبیرخانهٔ شورای‌عالی اطلاع‌رسانی در ادامهٔ فعالیتهای مربوط تلاش دارد تا با تهیه، ترجمه و تألیف مطالب فنی در محیط مناسب نسبت به تقویت دانش موجود کشور در قلمروی فناوری اطلاعات اقدام نماید. کتاب حاضر از جمله اسناد بسیار مفید، جامع و متأخر در قلمرو امنیت فناوری رایانه‌ای است که به دست‌اندرکاران ICT کشور هدیه می‌گردد.

نصرالله جهانگرد
دبیر شورای‌عالی اطلاع‌رسانی و
نماینده ویژه رئیس جمهور

یادداشت مترجمین

استفادهٔ درست از اطلاعات صحیح، یکی از نیازهای بسیار مهم برای دستیابی سازمانها به اهداف سازمانی است و قابلیت اطمینان، یکپارچگی و در دسترس بودن این اطلاعات، از مشخصه‌های بسیار مهم در کارآیی آنها هستند. مزایای ذخیره‌سازی اطلاعات بصورت الکترونیکی کاربرد وسیع رایانه‌ها در اهداف تجاری را ناگزیر کرده و استفاده از شبکه‌های رایانه‌ای و بویژه اینترنت، تغییرات اساسی را در روند کسب و کار بوجود آورده و باعث شده که حجم بسیار زیادی از اطلاعات تنها به اندازهٔ یک سر انگشت با ما فاصله داشته باشند؛ و ناگفته پیدا است که در این محیط پیچیده با این ارتباطات وسیع، مخاطرات گسترده‌ای سیستمهای رایانه‌ای، سیستمهای اطلاعاتی، و فعالیتها و زیرساختهای حیاتی وابسته به آنها را تهدید می‌کنند.

در دنیای امروز، اعتبارات مالی بیشتر و بیشتر بصورت الکترونیکی جابجا می‌شوند، اطلاعات مختلف با حساسیتهای کم و زیاد از طریق شبکه‌ها منتقل می‌شوند، سامانه‌های رایانه‌ای با سرعت بسیار زیادی پیچیده‌تر و مرتبط‌تر با دنیای بیرونی می‌گردند، و ابزارهای سادهٔ نفوذ و بهره‌برداری از آسیب‌پذیریها بیش از هر زمان دیگری در دسترس ماجراجویان و جنایتکاران دنیای مجازی قرار دارد؛ و هریک از این عوامل خود به تنهایی دلیل محکمی برای جدی گرفتن موضوع امنیت است.

اکثر قریب به اتفاق سازمانها در معرض انواع تهدیدات داخلی و خارجی خرابکاران هستند؛ تهدیداتی چون دستکاری اطلاعات مرجع و یا سرقت اطلاعات حیاتی و سرمایه‌های اطلاعاتی. در چنین شرایطی، عواملی که می‌توانند از مزایای سیستمها به شمار روند (مثل سرعت و قابلیت دسترسی بالا)، اگر تحت کنترل نباشند ممکن است باعث بروز آسیب‌پذیری شوند و سوء استفادهٔ افراد بدنیت از آنها به نفوذ و خرابکاری، کلاهبرداری، و یا اخاذی بیانجامد. علاوه بر این، مشکلات طبیعی و خطاهای غیرعمدی که توسط کاربران رایانه‌ای رخ می‌دهد، درصورت فقدان روالهای صحیح برای حفاظت از اطلاعات می‌تواند نتایج مخربی به بار آورد.

در کنار همهٔ این مسائل، موضوع جرائم سازمانیافتهٔ دنیای مجازی بر پیچیدگی کار دولتها برای تأمین امنیت زیرساختهای حیاتی خدمات عمومی می‌افزاید، و اهمیت سوء استفاده از منابع دولتی، اهمیت پرداختن صحیح و مؤثر آنها به موضوع امنیت را دو چندان می‌کند. آخرین آمارهای جهانی از رخدادهای پایگاههای وب دولتی و تجاری که توسط ویروس، کرم و حملات تخریب سرویس بوقوع پیوسته، آسیب‌پذیری این سیستمها را به خوبی به تصویر می‌کشد. طبق تخمین دستگاههای امنیتی ایالات متحده (که بعنوان پیشرو در حوزهٔ فناوریهای اطلاعات و ارتباطات شناخته می‌شود)، تنها در سال ۲۰۰۳ ضررهای ناشی از خدشه‌دار شدن امنیت سازمانها بالغ بر ۱۰ میلیارد دلار برآورد شده است.

با این اوصاف، تدوین و اجرای تدابیر امنیتی در قبال این تهدیدات گسترده، ضرورتی اجتناب ناپذیر برای سازمانها محسوب می‌شود. تدابیر مناسب می‌توانند احتمال وقوع مخاطرات را به حداقل برسانند، درصورت وقوع آنها میزان خسارتهای وارده را در حد بسیار ناچیزی نگه دارند، و قابلیت واکنش سریع و مؤثر بوجود آورند تا سازمانها برای ترمیم خسارتها از فرآیندهای از پیش تعیین-شده استفاده کنند تا بهره‌وری و ایمنی اطلاعات افزایش یابد و کسب و کار با خیالی آسوده‌تر تداوم یابد.

"راهنمای امنیت فناوری اطلاعات" پس از درک ضرورت پرداختن به موضوع امنیت، به سفارش بانک جهانی و توسط گروه infoDev (یکی از زیرمجموعه‌های بانک جهانی) و به عنوان تلاشی برای ارتقای سطح امنیت فناوری اطلاعات در کشورهای عضو در این نهاد بین‌المللی تدوین و برای اولین‌بار در اجلاس نخست سران جامعهٔ اطلاعاتی (WSIS) در سوئیس، در دسامبر سال ۲۰۰۳ میان شرکت‌کنندگان توزیع شد. محتویات این کتاب حاصل بررسی کتابها، مقالات، رساله‌ها، و مستندات تخصصی زیادی از کارشناسان و متخصصین این حوزه در سراسر دنیا است. فهرست کاملی از این مراجع در بخش ششم (پیوستها) آمده است که خوانندگان محترم می‌توانند با مراجعه به آنها از آخرین نکات و موضوعات نیز آگاهی یابند.

کتاب حاضر علاوه بر اینکه مجموعه‌ای از تعاریف و راهکارهای امنیت عمومی را ارائه کرده، جنبه‌های فنی مدیریتی آنها را نیز مدنظر قرار داده است و در متن اولیه و همچنین ترجمهٔ آن تلاش شده تا حد امکان مطالب بگونه‌ای عنوان شوند که فهم و درک آنها نیاز به دانش اختصاصی در این حوزه نداشته باشد و بتواند به کار جامعهٔ گسترده‌ای از کاربران فناوری اطلاعات (خصوصاً مدیران) بیاید، و لذا می‌توان سرفصلهایی از آنرا در سمینارهای آموزشی دوره‌های کوتاه‌مدت مورد استفاده قرار داد.

در سطح جهانی، کتابهای متعددی در حوزهٔ امنیت فناوری اطلاعات و ارتباطات منتشر و بازگی تعدادی از آنها نیز توسط مترجمان باتجربه و یا جوان به فارسی ترجمه شده، اما معمولاً چون به موضوعی تخصصی در زمینهٔ امنیت پرداخته‌اند، فاقد نگاه کلان و مدیریتی به این موضوع هستند. کتابی که پیش روی شما است، با نگاه کلان به موضوع امنیت، کوشیده مفاهیم مطرح در هریک از حوزه‌های آنرا شرح دهد، و آنجا که لازم بوده از بررسی جنبه‌های فنی نیز غافل نشده، هرچند هیچگاه آنچنان وارد مسائل فنی نشده که کلان‌نگری خود را از دست داده باشد، و اینکار را به کتابهای تخصصی امنیت واگذار کرده است.

مترجمان این اثر همواره کوشیده‌اند تا در انتقال مفاهیم و نکات این کتاب، حفظ امانت نمایند و هیچگاه معانی را فدای الفاظ نکرده و در بسیاری از موارد واژه‌سازی یا معادل‌سازی نموده‌اند، که کاری طاقت‌فرسا و مسئولیت‌آور است. سایر عناوینی که برای آنها معادل فارسی یافته و یا ساخته نشده نیز بصورت اصلی در ترجمه تکرار شده‌اند. امیدواریم خوانندگان محترم اعم از صاحبنظران، اساتید دانشجویان، و علاقه‌مندان با ارائه پیشنهادات و انتقادات خود ما را در رفع لغزشها و کاستیهای احتمالی این کتاب آگاه سازند تا در صدد رفع آنها برآییم.

برای جلوگیری از سردرگمی خوانندگانی که به تازگی به مقولهٔ امنیت اطلاعات علاقه‌مند شده‌اند و هنوز با اصطلاحات امنیتی و معادلهای رایج آنها آشنایی چندانی ندارند، در انتهای کتاب فهرستی از لغات و اصطلاحات رایج امنیتی که در کتاب از آنها استفاده شده و نیز معادل فارسی بکاررفته برای آنها تعبیه شده است. در صفحه‌آرایی کتاب نیز از نسخهٔ اصلی کتاب الگوبرداری شده و جز بخش پنجم – که بدلیل وجود متون فنی و متن‌برنامه زیاد، از تمام فضای صفحه برای متن استفاده شده است – در سایر بخشها از صفحه‌آرایی دوستونی استفاده شده است.

در پایان بر خود لازم می‌دانیم از خانم مریم افتخاری و آقایان محمدمهدی جاقوری، افشین لامعی، و نیما لطفی که در تهیهٔ این اثر متحمل زحماتی شدند، کلیهٔ اساتید و صاحبنظرانی که با ارائه نظرات کارشناسی و راهگشای خود به ما در انجام اینکار دلگرمی دادند، کلیهٔ همکارانی که به نوعی در تهیه و تنظیم این اثر نقش داشتند، و نیز دبیرخانهٔ شورای عالی اطلاع‌رسانی که زحمت چاپ و نشر این کتاب را عهده‌دار شد صمیمانه تشکر نماییم.

امید آنکه این مکتوب بتواند اثری هرچند جزئی در سیر پیشرفت و توسعهٔ کشور در مسیر نیل به ایرانی آباد، آزاد و سرفراز مؤثر افتد.

گروه مترجمین
تابستان ۱۳۸۴

دیباچه

کلیهٔ اعتبارات مربوط به تهیه و تدوین کتاب حاضر از *طرح infoDev گروه بانک جهانی*[1] تأمین شده است. طی سالهای اخیر موضوع *امنیت فناوری اطلاعات*[2] به اهمیتی ویژه دست یافته و به همین دلیل مورد توجه *گروه مشاورهٔ فنی infoDev*[3] واقع شده است. در اینجا بر خود لازم می‌دانیم که مراتب تشکر و امتنان خود را به دلیل بذل توجه *دبیرخانهٔ ایالتی امور اقتصادی سوئیس* (SECO)[4] نه‌تنها بخاطر تأمین اعتبار این پروژه، بلکه بخاطر درک فوریت مسئله و به ثمر رساندن این کتاب اعلام نمائیم.

فناوری اطلاعات و ارتباطات (ICT)[5] نقش مهمی در توسعهٔ اقتصادی و اجتماعی ایفا می‌کند، ولی این نکته را نیز نباید از نظر دور داشت که در یک محیط ناامن و غیر قابل اطمینان، استفادهٔ مؤثر از فناوری اطلاعات و ارتباطات ناشدنی است. بنابراین امنیت فناوری اطلاعات دارای نقشی اساسی و تعیین‌کننده در ایجاد شرایط لازم برای پیاده‌سازی موفق طرح‌های ملی فناوری اطلاعات و ارتباطات، دولت الکترونیکی، تجارت الکترونیک و اجرای پروژه‌هایی در زمینه‌های آموزش و پرورش، بهداشت یا امور مالی و اعتباری است.

امنیت فناوری اطلاعات موضوع پیچیده‌ای است و تقریباً همگام با فناوری در حال تکوین است. مؤلفین در این کتاب توانسته‌اند بهترین راهکارها و پیشنهادات را – مستقل از فناوری – برای محیط‌های ویژهٔ فناوری اطلاعات ارائه دهند. خوانندگان همچنین می‌توانند با مراجعه به پایگاه وب *www.infodev-security.net* به اطلاعات به‌روز و مناسب دست یابند و از طریق این جریان اطلاع‌رسانی ثابت، از پیشرفت‌های جدید در زمینهٔ امنیت فناوری اطلاعات باخبر شوند. با توجه به اینکه مطالب ارائه‌شده در این کتاب لزوماً دیدگاه‌های infoDev یا گروه بانک جهانی را منعکس نمی‌کند، بنظر ما استفاده از این کتاب در کنار پایگاه وب مربوط به آن می‌تواند کمک بزرگی به فهم موضوعات مرتبط با امنیت فناوری اطلاعات در سراسر جهان نماید.

کتاب حاضر متشکل از پنج بخش است که هریک از آنها می‌تواند بصورت جداگانه مورد مطالعه قرار گیرد. پس از مقدمه‌ای کوتاه بر عناوین عمومی امنیت فناوری اطلاعات، به مطالب و مباحثی برخورد خواهیدکرد که برای کاربران انفرادی، سازمانهای کوچک و متوسط، دولت، و راهبران فنی مناسب هستند. هرچند بیشتر پژوهشها و مقالات منتشر شده دربارهٔ امنیت فناوری اطلاعات در کشورهای توسعه‌یافته پیدا می‌شود، ولی تلاش مؤلفین بر این بوده که خط‌مشی‌های عملی و کارآمدی ارائه دهند که در کشورهای درحال توسعه نیز قابل استفاده باشد.

امیدواریم انتشار این کتاب و آغاز بکار پایگاه وب آن نقطهٔ آغاز یک فرآیند تعاملی از پیشرفت همزمان راهکارها و فناوری باشد؛ و در این راه آنچه بیش از همه اهمیت دارد این است که خوانندگان محترم کتاب، شیوه و راهکارهای مناسب و کارآمد خود را در اختیار دیگران نیز قرار دهند.

Mohesn A. Khalil : مدیر بخش فناوری اطلاعات و ارتباطات بین‌المللی – گروه بانک جهانی

Burno Lanvin : مدیر برنامهٔ infoDev – گروه بانک جهانی

Michel A.Maechler : مدیر تقسیم وظایف گسترش اطلاعات، کارشناس ارشد انفورماتیک – گروه بانک جهانی

---

1 *infoDev Program of the World Bank Group*
2 *IT Security*
3 *infoDev Technical Advisory Panel*
4 *State Secretariat of Economic Affairs of Switzerland*
5 *Information & Communication Technology*

پیش‌درآمد

سیر پیشرفت فناوری اطلاعات و ارتباطات و نوآوریهای حاصل از آن موجب افزایش چشمگیر بهره‌وری و پیدایش انواع جدیدی از کالاها و خدمات شده است. با بهبود روزافزون قدرت، ظرفیت و قیمت تجهیزات میکروالکترونیکی که به رشد سالانهٔ تقریباً ۳۰ درصدی بهره‌وری نسبت به قیمت منجر شده، امکان استفاده از این فناوری برای همه میسر شده است. امروزه ما در دنیایی زندگی می‌کنیم که پردازش اطلاعات در آن ارزان و هزینه‌های ارتباط تلفنی رو به کاهش است و جهان بطور فزاینده‌ای در تبادل و تعامل می‌باشد.

اما فراهم شدن امکانات فنی جدید تنها باعث پیدایش محصولات نوین و راههای بهتر و کارآمدتر برای انجام امور نشده، بلکه در کنار آن امکان سوء استفاده از فناوری را نیز افزایش داده است. فناوری اطلاعات و ارتباطات نیز همانند سایر فناوریها حالت ابزاری دارد و می‌توان آنرا بگونه‌ای مورد استفاده قرار داد که برای همگان مفید باشد و یا به نحوی از آن استفاده کرد که نتایج خطرناکی به بار آورد. عامل سرعت در فناوری اطلاعات و ارتباطات چیزی در حدود میکروثانیه است که باعث می‌شود اطلاعات غیرقابل مشاهده با چشم غیرمسلح، تحت کنترل نرم‌افزار تهیه‌شده توسط افراد جابجا گردد. در چنین فضایی اعمال غیرقانونی و مخرب آنقدر سریع صورت می‌گیرد که می‌تواند غیرقابل شناسایی باشد - هرچند شناسایی آن غیر ممکن نیست.

مشکلات مربوط به امنیت سیستمهای اطلاعاتی، فرآیندهای وابسته به آنها و ذخیره و ارسال اطلاعات به شکل الکترونیکی مسائل تازه‌ای نیستند. سیستمهای تجاریِ رایانه‌ای نزدیک به پنجاه سال قدمت دارند. سیستمهای بانکداری نیز انتقال الکترونیکی پول را تقریباً در همان زمان آغاز کرده‌اند.

در این سیستمهای تجاری، برای ارتکاب جرم از طریق نفوذ به شبکه‌های رایانه‌ای و سیستمهای مالی انگیزه‌های قوی وجود دارد. در واکنش به افزایش احتمال انجام فعالیتهای تبهکارانه و برای تهیهٔ معیارهای امنیتی قوی‌تر در عرصهٔ ارتباطات و پردازش، طرحهای تحقیقات و توسعه‌ای اطلاعات آغاز شده است.

در نیم‌قرن اخیر بسیاری از مسائل تغییر کرده‌اند. انقلاب رایانه‌های شخصی که در اواسط دههٔ ۷۰ میلادی شروع شد درحال حاضر موجب شده رایانه‌هایی با اندازه و قدرتی قابل ملاحظه در دسترس صدها میلیون نفر قرار داشته باشند. علاوه بر آن اینترنت و دیگر انواع شبکه‌های شخصی ارتباطات بین رایانه‌ای را میان بسیاری از مردم امکانپذیر ساخته‌اند. بیست و پنج سال پیش کار با رایانه و برقراری ارتباطات عموماً توسط تعداد کمی از کارشناسان این رشته صورت می‌پذیرفت؛ اما امروزه صدها میلیون رایانه برای پردازش هرگونه اطلاعات قابل تصوری بکار می‌روند و توسط یک شبکهٔ ارتباطی قوی بنام اینترنت به هم متصل می‌شوند. این شبکه موجب گسترش ارتباطات مردمی از طریق پست الکترونیکی و قابلیت ارسال پیام فوری شده و همچنین امکان دسترسی آسان و نسبتاً ارزان به مفاهیم دیجیتالی و اسناد تجهیزات فنی و محصولات درحال ساخت را بوجود آورده است. بدیهی است که به تناسب پیشرفت فناوری، مشکلات نیز بیشتر می‌شود. عمدهٔ کاربران شبکه‌های رایانه‌ای دههٔ ۷۰ میلادی را کارشناسان حرفه‌ای رایانه تشکیل می‌دادند؛ حال آنکه امروز بیشتر کاربران از افراد غیرحرفه‌ای هستند و لذا ممکن است عدم اطلاعات کافی آنان باعث شود که از بسته‌های نرم‌افزاری ایمن استفادهٔ مناسب نکنند و درنتیجه نفوذگران و تبهکاران رایانه‌ای صرفنظر از محل جغرافیایی خود و یا کاربر بتوانند به سیستم حمله و از آن سوء استفاده نمایند.

اگر در منزل و یا محل کار خود از رایانه استفاده می‌کنید مسئولیت حفاظت از اطلاعات آن بر عهدهٔ شما است. این کتاب به شما کمک می‌کند که جزئیات فنی و نحوهٔ کارکردن با یک رایانه یا شبکه‌ای از رایانه‌های متصل به هم را بیاموزید. تلاش برای حفظ امنیت وظیفهٔ هر فرد است. این فرد می‌تواند یک کاربر عادی، کارشناس فنی، راهبر سیستم، راهبر شبکه، و مدیر یک سیستم یا شبکه در سازمان باشد. توجه به اهمیت امنیت باعث می‌شود اقدامات ضروری و اطمینان‌بخشی برای حفاظت از سیستمها صورت پذیرد و استفاده از مجموعه‌ای مؤثر از سیاستهای امنیتی، گام مهمی در جهت اطمینان از این مسئله است. در آنصورت در بیشتر

موارد رایانه‌ها و اطلاعات شما از دسترسیهای غیرمجاز ایمن خواهند بود و خواهید توانست اطلاعات خود را بصورت امن در شبکه با سایرین مبادله کنید.

این کتاب زمانی‌تهیه شد که استفاده از فناوری اطلاعات و ارتباطات در توسعهٔ اقتصادی- اجتماعی به اوج خود رسیده بود و علاوه بر آن به مدت ۴۰ سال یا بیشتر در غالب طرحهای منطقه‌ای یا عملیاتی که توسط مراکز کمک‌رسانی دومنظوره یا چندمنظوره اجرا می‌شدند بکار می‌رفت. این باور که فناوری اطلاعات و ارتباطات یک موضوع مهم و حیاتی برای آغاز بسیاری از فعالیتهای توسعه‌ای است موضوعی نسبتاً تازه می‌باشد و شروع آن به راه‌اندازی شبکه جهانی اینترنت در اوایل دههٔ ۹۰ میلادی باز می‌گردد. این موضوع برای اولین بار در یک مؤسسهٔ چندمنظوره توسط برنامهٔ infoDev در گروه بانک جهانی در سال ۱۹۹۵ میلادی رسماً اعلام شد و از پشتیبانی فکری رئیس وقت بانک جهانی جیمز *ولفسن*[1] برخوردار بود که بر اهمیت به‌اشتراک‌گذاری اطلاعات برای نیل به اهداف توسعهٔ اقتصادی- اجتماعی تأکید زیادی داشت. از آن زمان به بعد خوش‌بینی نسبت به توسعهٔ اقتصادی- اجتماعی بیشتر شد که بخشی از آن به دلیل توسعهٔ فناوریهای ارزان در سراسر جهان بود.

در سال ۲۰۰۱ کشورهای عضو گروه G8، *کمیتهٔ کاری فرصتهای دیجیتالی* (DOT)[2] را پایه‌ریزی کردند. کمیتهٔ DOT نتایج کار خود را طی گزارشی ارائه نمود و خواستار قرارگرفتن ۹ موضوع در *طرح اجرایی ژنو*[3] شد که همهٔ آنها در اجلاس سران ژنو در سال ۲۰۰۱ به تأیید و امضای رهبران گروه G8 رسیدند. اعضای اصلی کمیتهٔ DOT سهامداران اصلی گروه G8 و دولتهای کشورهای درحال توسعه، بخشهای خصوصی و غیرانتفاعی و همچنین انبوهی از سازمانهای بین‌المللی هستند. گزارش مزبور شامل ۷ بند عملیاتی بعنوان موضوعات حیاتی برای ایجاد جامعهٔ اطلاعاتی می‌باشد:

۱) پشتیبانی از سیاستها
۲) ارتقا و بهبود دسترسی
۳) توسعهٔ منابع انسانی
۴) پرورش کارآفرینان و فعالیتهای کارآفرینی
۵) مشارکت کشورهای درحال توسعه در کنفرانسهای بین‌المللی در زمینهٔ فناوری اطلاعات
۶) کاربرد فناوری در بهداشت و سلامت
۷) نرم‌افزارهای کاربردی و مفاهیم محلی

یکی از نتایج این گزارش ایجاد *کمیتهٔ اجرایی ICT دبیرکل سازمان ملل*[4] بود و از دیگر نتایج آن می‌توان به تشکیل مؤسسهٔ *پیشگامان فرصتهای دیجیتال بین‌المللی*[5] با استفاده از اعتبار *UNDP*[6]، *بنیاد آکسنچر*[7] و *بنیاد مارکل*[8] اشاره کرد. همچنین درحال حاضر مؤسسات دومنظوره در طرحهای توسعه‌ای خود توجه روزافزونی به فناوری اطلاعات و ارتباطات نشان می‌دهند. پس از آن ITU و UNESCO نیز طرحهایی را برای برگزاری دو اجلاس جهانی با نامهای *اجلاس جهانی سران جامعهٔ اطلاعاتی* (WSIS)[9] در ژنو (دسامبر ۲۰۰۳) و تونس (آوریل ۲۰۰۵) ارائه کردند.

فناوری اطلاعات و ارتباطات می‌تواند به شکل غیرمستقیم بسیاری از فعالیتها را در دستیابی به *اهداف توسعه‌ای هزاره* (MDG)[10] پشتیبانی کند. سیاستهای اصلی تأمین امنیت فناوری اطلاعات و پیاده‌سازی آنها در یک کشور باعث تقویت جریان سرمایه‌گذاری مستقیم خارجی در آن کشور خواهد شد و این سرمایه‌گذاریها به فراهم شدن اعتبار برای تأمین امنیت بسیاری از زیرساختهای اقتصادی می‌انجامد.

حال این سؤال پیش می‌آید که چرا به این کتاب که در وهلهٔ اول برای خوانندگان در کشورهای درحال توسعه نگاشته شده نیاز است. در پاسخ به این پرسش باید گفت که اصول امنیتی همواره یکسانند؛ مستقل از اینکه شما در یک کشور توسعه‌یافته، درحال توسعه یا توسعه‌نیافته باشید؛ چراکه فناوریها و تهدیدات مربوط به آنها ممکن است از هر گوشهٔ جهان ظاهر شوند. البته راههای گوناگونی برای ایمن کردن رایانه‌ها و شبکه‌ها وجود دارد که بی‌تردید در کشورهای درحال توسعه همیشه در دسترس و ارزان نیستند.

1 *James Wolfensohn*
2 *Digital Opportunity Taskforce Group*
3 *Genoa Plan of Action*

4 *U.N. Secretary General's ICT Task Force*
5 *Global Digital Opportunities Initiative*
6 *United Nations Development Program*
7 *Accenture Foundation*
8 *Markle Foundation*
9 *World Summit on Information Society*
10 *Millennium Development Goals*

ابتدا ذکر این نکته مهم است که کاربران و راهبران رایانه در کشورهای توسعه‌یافته دسترسی بسیار زیادی به اطلاعات کاربردی و تکنیکی دارند که می‌تواند در زمینه‌های مختلف کاری به آنها کمک نماید. برای مثال کتابفروشی‌ها و کتابخانه‌های زیادی وجود دارند که از رایانه استفاده می‌کنند و لذا درخواست کمک از افراد هم‌صنف دیگر به راحتی امکانپذیر می‌باشد. زمانی که یک رایانه یا شبکه دچار اشکال می‌شود، مجموعه‌ای غنی از کانالهای اطلاعاتی وجود دارد که اخبار و اطلاعات امنیتی از طریق آنها ارسال می‌گردد. سازمانهایی که از رایانه‌ها و شبکه‌ها استفاده می‌کنند دارای *مراکز کمک‌رسانی*[11] هستند که توسط متخصصین فنی اداره می‌شوند و قادر به جلوگیری از کاربرد سوء منابع سازمانی و تأمین حفاظت آنها می‌باشند.

کاربران و راهبران فنی در کشورهای درحال توسعه معمولاً فاقد توانایی ارائه این سطح از پشتیبانی هستند. تعداد کاربران اندک است و به هشدارها و راه‌حلهای ارائه‌شده نیز توجه نمی‌شود. سازمانهایی که از رایانه استفاده می‌کنند غالباً دارای بخش ستادی کوچکی هستند و لذا توانایی نظارت بر منابع فنی داخلی خود را ندارند. بسیاری از اوقات این عدم توجه و ناتوانی به دلیل عدم وجود اطلاعات و دانش کافی دربارهٔ سیستمهای رایانه‌ای و امنیت شبکه است، و گروههایی که اصول اساسی را درک کرده‌اند نیز معمولاً در فهم چگونگی سازگارسازی راهکارهای فنی با شرایط متغیر و غیرقابل پیش‌بینی این محیط مشکل دارند.

خدمات پس از فروش در گذشته بصورت نامحدود برای رایانه‌هایی که کم‌تعداد و گرانقیمت بودند درنظر گرفته می‌شد؛ اما درحال حاضر با توجه به حجم انبوه رایانه‌ها در بازار نمی‌توان بسادگی چنین خدماتی را ارائه کرد. فروشگاهها و مراکز خدمات تعمیرات رایانه معمولاً از مشکلاتی که در سایر نقاط دنیا بوجود می‌آیند مطلع نیستند و درنتیجه کاربران و راهبران به قربانیان توسعهٔ اطلاعات مربوط به امنیت فناوری تبدیل می‌شوند.

نقص امنیتی شبکه در همهٔ کشورها اتفاق می‌افتد و حتی ممکن است موجب تحت فشار قرار گرفتن دولتها نیز بگردد. معمولاً بسیاری از این نقصها گزارش نمی‌شوند؛ چراکه اطلاع عموم مردم از آنها می‌تواند نتایج نامطلوبی به بار آورد. دولتها و سازمانهای موجود در کشورهای توسعه‌یافته عموماً توانایی مقابله با چنین نقصهایی را دارند، ولی نتایج ناشی از بروز نقصها و اشکالات امنیتی در کشورهای درحال توسعه می‌تواند بسیار وخیم‌تر از کشورهای توسعه‌یافته باشد. در کنار همهٔ این موارد، بازارها، سازمانها و دولتهای کشورهای درحال توسعه به دلیل عدم توجه به عواقب ناشی از نفوذهای رایانه‌ای در حجم وسیع، عدم توانایی تحلیل ضررهای مالی ناشی از این حملات، و نیز نداشتن تخمین مناسب از زمان لازم برای ترمیم خسارات وارده (البته اگر این خسارات قابل ترمیم باشند) تمایل چندانی به رفع نقایص امنیتی ندارند.

کشورهای درحال توسعه باید تأمین امنیت را بعنوان اولویت اصلی خود درنظر بگیرند، چراکه خطر فعالیتهای تبهکارانه بیشتر متوجه مکانهایی است که از کنترل کافی برخوردار نبوده و ناامن هستند. تجارت الکترونیکی در کشورهایی که امنیت فناوری اطلاعات در آنها کمتر تأمین شده اهداف جذاب‌تری برای حمله هستند. کدام سازمان کوچک یا متوسط است که علیرغم به سرقت رفتن اطلاعات محرمانهٔ مشتریان، فایلهای تجاری و یا دستکاری شدن اطلاعات کلیدی سازمان همچنان بتواند پابرجا بماند؟ کشورهای درحال توسعه باید ظرفیت منابع انسانیِ آموزش‌دیده و زیرساختهای فناوری خود را بهبود بخشند تا اهداف آسانی برای حملهٔ تبهکاران فضای رایانه‌ای نباشند. در این کتاب بحثهای بسیاری دربارهٔ ماهیت موضوع امنیت مطرح شده است؛ چراکه در مورد نیاز به تأمین امنیت دیدگاه‌های متفاوتی وجود دارد. افرادی که در مورد داده‌ها نگرانی دارند به این مسئله بعنوان یک موضوع در حوزهٔ امنیت اطلاعات می‌نگرند؛ کسانیکه با مکانیزمهای فنیِ ذخیره و ارسال اطلاعات سر و کار دارند این مبحث را از دید امنیت سیستم و شبکه می‌بینند؛ حال آنکه دیگرانی که به تجارت مشغول هستند به آن بعنوان یک حوزهٔ جدید در تجارت و عموماً تحت عنوان امنیت الکترونیکی نگاه می‌کنند.

با توجه به این مسائل ما ترجیح داده‌ایم تمام مباحثی که در مقوله "امنیت فناوری اطلاعات" می‌گنجد را ارائه کنیم و از این طریق به تمامی مکانیزمهای ذخیره و پردازش و ارسال اطلاعات، سخت‌افزار، نرم‌افزار، و تسهیل ارتباطات، با یک نگاه ویژه به مسئله امنیت خود اطلاعات بپردازیم. این مسئله

11 *Help Centers*

حائز اهمیت است که هم اطلاعات و هم مکانیزمهای پردازش آن باید از سوء استفاده مصون باشند.

ما تعمداً در این کتاب توجه خود را به رایانه‌ها، نرم‌افزارها و شبکه‌ها محدود کرده‌ایم؛ چراکه منابع غنی و متعددی برای آگاهی از جزئیات مسائل دیگر نظیر تلفن ثابت و همراه که در ارتباط تنگاتنگ با این مسائل هستند و در اینجا به آنها پرداخته نشده وجود دارد. با نزدیکتر شدن فناوریهای تلفنی و رایانه‌ای به یکدیگر، چنین مسائلی نیز اهمیت بیشتری پیدا می‌کنند. با پیدایش Voice over IP و ENUM، پروتکلهای تلفن دیجیتالی نیز کاربرد روزافزونی می‌یابند و با پیدایش فناوریهای 3G بتدریج به مسائلی چون امنیت در آنها نیز باید توجه کرد.

این کتاب به نحوی تدوین شده که در کشورهای درحال توسعه نیز با هزینه‌ای اندک در دسترس باشد. هدف از انتشار این کتاب این نیست که به تیراژ بالایی از آن دست یابیم، بلکه بنا بر این است که مفاد کتاب در یک پایگاه وب جهانی ارائه گردد که از دو لحاظ پویا باشد: اول اینکه مطالب آن تا حد امکان به‌روزرسانی‌شده باشد، و دوم اینکه اطلاعات مفید و مناسبی به خوانندگانی که بدنبال کسب اطلاعاتی دربارهٔ امنیت فناوری اطلاعات هستند ارائه کند.

مطالب این کتاب به پنج بخش مختلف تقسیم شده که هریک مناسب گروه خاصی از خوانندگان هستند. لازم به ذکر است که در بخشهای مختلف کتاب گاهی می‌توان مطالب مشترک و تکراری پیدا کرد، چراکه با اینکار بسیاری از خوانندگان می‌توانند تنها بخشی از کتاب را برای خواندن انتخاب کنند که به کار آنها می‌آید. بعضی بخشها – خصوصاً آنهایی که به تشریح امنیت و کاربران رایانه‌ای می‌پردازند – را می‌توان بطور مستقل منتشر و میان کاربرانی که به آنها نیاز دارند توزیع نمود.

در تهیه و تدوین این کتاب ناچار به ایجاد توازن میان اصول کلی، نمونه‌های ویژه، و اطلاعات عملی بوده‌ایم و امیدواریم که توازن ایجادشده از تناسب لازم برخوردار باشد. اگرچه با پیشرفت و تکامل فناوری، جزئیات فنی نیز تغییر خواهند کرد، اما این اصول همواره ثابت خواهند بود و خوانندگان از نظر سیاست و مدیریت و همچنین از نظر فنی قادر به فهم آسان آنها می‌باشند. اگر این اصول بدقت درک شوند آنگاه راه‌حلهای فنی بسادگی در دسترس قرار خواهند گرفت.

خواننده باید توجه داشته باشد که مؤلفین برای مقولهٔ امنیت و رایانه از اصطلاحات مختلفی استفاده کرده‌اند. بطور کلی مقولهٔ امنیت فناوری اطلاعات به موضوعات زیر اشاره دارد:

۱) **امنیت رایانه:** امنیت از نظر فنی در ماشینها، نرم‌افزار، داده‌ها و شبکه‌ها. از این اصطلاح بیشتر در بخشهای دوم و پنجم استفاده شده که بیشتر بر روی ابعاد فیزیکی، زیرساختی و فنی امنیت فناوری تأکید دارند.

۲) **امنیت سایبر**[12]: امنیت فناوری اطلاعات وابسته به سیاست دولتها. این اصطلاح عموماً توسط مؤسسات دولتی و سیاستگذاران ملی در اسناد، قوانین و پروژه‌های تحقیقاتی استفاده می‌شود و کمابیش مترادف با "امنیت اینترنت" است (اصطلاحی که در این کتاب به آن اشاره‌ای نشده، اما گاهی اوقات در مراجع دیگر به چشم می‌خورد). هر دو عبارت به جوانب امنیت شبکه و اصول سیاستگذاری شبکه‌ها مثل تعریف حریم خصوصی، جرائم سایبر، تجارت و ارتباطات جهانی اشاره دارند. تفاوت این دو اصطلاح چندان زیاد نیست؛ بلکه همانطور که در بسیاری از فصلهای این کتاب می‌توان دید، امنیت رایانه‌ها، شبکه‌ها و داده‌ها تا حد زیادی با مفاهیم روزمرهٔ امنیت در فضای سایبر به هم گره خورده‌اند.

در دنیای سریع و درحال پیشرفت امروز، تدوین کتاب راهنما در معرض این خطر است که اندکی پس از انتشار از رده خارج و قدیمی شود. برای به‌روز نگهداشتن محتویات این کتاب تمامی بخشهای آن در یک پایگاه وب به آدرس *www.infodev-security.net* موجود هستند تا هریک را بتوان در آینده به روزرسانی نمود. خوانندگانی که مایل به اضافه کردن مطالب مفید در به‌روزرسانی پایگاه وب باشند می‌توانند پیشنهادات خود را به آدرس الکترونیکی contact@infodev-security.net ارسال نمایند.

تدوین این کتاب بدون حمایت تعدادی از افراد و مؤسسات ویژه و مهم هیچگاه ممکن نبود، از جمله *سیمسون گارفینکل*[13]، که راهنماییهای مهمی در تدوین ساختار اولیهٔ این کتاب نمود و پس از آن در شناسایی و هماهنگ‌سازی قسمتی از تیم تهیه‌کنندگان کتاب کمک کرد. انتشار این

12 *Cyber-Security*
13 *Simson Garfinkel*

کتاب راهنما بدون راهنمایی و کمک او میسر نمی‌شد. *برونو لنوین*[14]، مدیر infoDev که اعتبارات زیادی برای تفهیم مناسبت و قدرت خلق اطلاعات و توزیع آن در زمینهٔ فناوری اطلاعات و ارتباطات اختصاص داد؛ همچنین *ژاکلین دوبو*[15]، *الی الوی*[16]، *تری ناکازل*[17] و *هریری برتادو*[18] که همگی از مدیران infoDev هستند. از تیم اوریلی که با پشتیبانی شرکت خود به نام *اوریلی و شرکا*[19] دو کتاب زیر را منتشر کردند نیز تشکر می‌کنیم: *امنیت اینترنت و کاربرد یونیکس*[20]، ویرایش سوم (سیمسون گارفینکل، *ژن اسپافورد*[21] و *آلن شوارتز*[22]، چاپ ۲۰۰۳) و *امنیت وب، محرمانگی و تجارت*[23] (سیمسون گارفینکل و ژن اسپافورد، چاپ ۲۰۰۲). این کتابها برای تکمیل بخشهای مهمی از این کتاب راهنما مورد استفاده قرار گرفته‌اند و چند بخش آنها نیز با کسب مجوز از نویسندگان و ناشران برای چاپ مجدد در این کتاب راهنما بکار رفته‌اند.

علاوه بر اینها شرکت اوریلی و شرکا در ده سال اخیر دهها هزار عنوان از کتابهای فنی خود را در اختیار مردم کشورهای درحال توسعه قرار داده است. خوانندگانی که وضعیت کتابها و دسترسی به مطالب منتشر شده در جهان درحال توسعه را دیده‌اند می‌دانند که مشارکت اورلی در سیر توانمندی علمی این کشورها جهت آشنایی، پخش و بهره‌برداری از اینترنت و لذا کاهش شکاف دیجیتالی چقدر مؤثر و حائز اهمیت بوده است.

بر خود لازم می‌دانیم از گردآورندگان کتابهای فوق‌الذکر برای کمک شایسته و مشتاقانه جهت استفاده از مطالب کتابهایشان در بخشهایی از این کتاب راهنما به گرمی تشکر کنیم. شور و اشتیاق آنان برای کمک به انتشار این کتاب راهنما بهترین نمونهٔ همکاری تخصصی و به‌اشتراک‌گذاری اطلاعات در تمدن نوین اینترنتی امروز است.

در اینجا لازم می‌دانیم از *تام کلرمن*[24]، متخصص ارشد *مدیریت مخاطرهٔ داده‌ها*[25] در تیم *امنیت خزانهٔ بخش سیاست عملیاتی بانک جهانی*[26] نیز تشکر نماییم. نوشته‌های وی در مورد *خدمات مالی الکترونیکی*[27]، *تهدیدات چندوجهی*[28] و *مدیریت خطر سیار*[29] در بخش سوم این کتاب مورد استفاده قرار گرفته‌اند.

ماکس اشنلمن[30] نمایندهٔ سوئیس در کمیتهٔ توسعهٔ اطلاعات در اجلاس چانگ کین[31] چین در سال ۲۰۰۲ نیز یکی از اولین کسانی بود که اهمیت و فایدهٔ دستنامهٔ امنیت فناوری اطلاعات در کشورهای درحال توسعه را تشخیص داد و پشتیبانیها و توصیه‌های او بود که به حمایت دولت سوئیس از infoDev برای انتشار این کتاب انجامید و ما در اینجا این پشتیبانی وی را مورد تقدیر قرار می‌دهیم.

مایکل مکلی[32] نیز گروهی از متخصصین فعال را برای تدوین مطالب این کتاب تشکیل داد و همین افراد بودند که پیشنهادات ارزشمندی برای افزایش دقت و تناسب نسخهٔ نهایی این کتاب ارائه کردند؛ و ما در اینجا از راهنماییهای سازندهٔ ایشان تشکر می‌کنیم؛ و همچنین مراتب تشکر و امتنان خود را به تمامی دست‌اندکاران و افرادی که به روند چاپ این کتاب کمک کردند اعلام می‌نماییم.

این کتاب نه مرجعی آموزشی برای سیستم‌عاملهای Unix، Windows یا Macintosh است و نه مرجعی برای آموزش راهبری سیستم؛ بلکه باید در کنار راهنماهای راهبری این سیستمها مورد استفاده قرار گیرد.

مدیریت تغییرات وسیع در سیستمهای رایانه‌ای ممکن است پشتیبانی از آنها را دچار مشکل کند، حتی اگر این تغییرات برای ارتقای سطح امنیت لازم باشند. برای راحتی خوانندگان به منابع اینترنتی بسیاری اشاره کرده‌ایم، ولی اگر خوانندگان از برنامه‌ها و *وصله‌های*[33] پیشنهادی موجود اینترنت استفاده می‌کنند باید جانب احتیاط را رعایت کنند؛ چراکه ممکن است بعد از ایجاد تغییرات در هسته[34]، معماری و یا دستورات سیستمها، ارزیابی تأثیرات امنیتی آنها در سطح کلان بسادگی

14 Bruno Lanvin
15 Jacquelin Dubow
16 Ellie Alavi
17 Teri Nachazel
18 Henri Bretadeau
19 O'Reilly & Associates
20 Practical Unix and Internet Security 3rd Edition
21 Gene Spafford
22 Alan Schwartz
23 Web Security, Privacy & Commerce
24 Tom Kellermann
25 Senior Data Risk Management Specialist
26 Integrator Group and Treasury Security Team of the Operations Policy Department
27 E-Finance
28 Blended Threats
29 Mobile Risk Management
30 Max Schnellmann
31 Chongqing
32 Michel Maechley
33 Patches
34 Kernel

میسر نباشد. اگر راه‌حلها و برنامه‌های فروشنده‌های مختلف بطور عادی پیاده‌سازی یا نصب شوند ممکن است در درازمدت سطح کلی امنیت تضعیف گردد؛ پس باید به سازگاری تجهیزات سیستم و کیفیت و اشتهار شرکتهایی که خدمات فنی و مشاوره‌ای ارائه می‌دهند نیز توجه کرد.

امیدواریم کتاب حاضر درک این موارد را برای شما آسان‌تر کند و مطمئن هستیم که خوانندگان نیز به بهبود کیفی محتویات آن در آینده کمک خواهند کرد.