

پیش درآمد

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 سالانه 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 ایزاری 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 تهیه شده 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 تجاری 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 تهیه معیارهای امنیتی قوی‌تر در عرصه 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 دهه 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 تصویری بکار می‌روند و توسط یک شبکه 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. عمده کاربران شبکه‌های رایانه‌ای دهه 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 استفاده مناسب نکنند و در نتیجه 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 عهده شما است. این کتاب به شما کمک می‌کند که جزئیات فنی و نحوه کارکردن با یک رایانه یا شبکه‌ای از رایانه‌های متصل به هم را بیاموزید. تلاش برای حفظ امنیت وظیفه 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

- ۴ پرورش کارآفرینان و فعالیتهای کارآفرینی
- ۵ مشارکت کشورهای درحال توسعه در کنفرانسهای بین‌المللی در زمینه فناوری اطلاعات
- ۶ کاربرد فناوری در بهداشت و سلامت
- ۷ نرم‌افزارهای کاربردی و مفاهیم محلی

یکی از نتایج این گزارش ایجاد کمیته اجرایی ICT دبیر کل سازمان ملل^۴ بود و از دیگر نتایج آن می‌توان به تشکیل مؤسسه پیشگامان فرصتهای دیجیتالی بین‌المللی^۵ با استفاده از اعتبار UNDP^۶، بنیاد آکسنچر^۷ و بنیاد مارکل^۸ اشاره کرد. همچنین درحال حاضر مؤسسات دامنظوره 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 جامعه اطلاعاتی (WSIS)^۹ در ژنو (دسامبر ۲۰۰۳) و تونس (آوریل ۲۰۰۵) ارائه کردند.

فناوری اطلاعات و ارتباطات می‌تواند به شکل غیرمستقیم بسیاری از فعالیتهای در دستیابی به اهداف توسعه‌ای هزاره (MDG)^{۱۰} 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 وهله اول برای خوانندگانی 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 گوشه 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.

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

این کتاب زمانی تهیه شد که استفاده از فناوری اطلاعات و ارتباطات در توسعه 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 دامنظوره 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 دهه ۹۰ میلادی باز می‌گردد. این موضوع برای اولین بار در یک مؤسسه چندمنظوره توسط برنامه infoDev در گروه بانک جهانی در سال ۱۹۹۵ میلادی رسماً اعلام شد و از پشتیبانی فکری رئیس وقت بانک جهانی جیمز ولفسن^۱ برخوردار بود که بر اهمیت به‌اشتراک‌گذاری اطلاعات برای نیل به اهداف توسعه اقتصادی-اجتماعی تأکید زیادی داشت. از آن زمان به بعد خوش‌بینی نسبت به توسعه اقتصادی-اجتماعی بیشتر شد که بخشی از آن به دلیل توسعه فناوریهای ارزان در سراسر جهان بود.

در سال ۲۰۰۱ کشورهای عضو گروه G8، کمیته کاری فرصتهای دیجیتالی (DOT)^۲ را پایه‌ریزی کردند. کمیته DOT نتایج کار خود را طی گزارشی ارائه نمود و خواستار قرارگرفتن ۹ موضوع در طرح اجرایی ژنو^۳ شد که همه آنها در اجلاس سران ژنو در سال ۲۰۰۱ به تأیید و امضای رهبران گروه G8 رسیدند. اعضای اصلی کمیته 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 جامعه اطلاعاتی می‌باشد:

- ۱ پشتیبانی از سیاستها
- ۲ ارتقا و بهبود دسترسی
- ۳ توسعه منابع انسانی

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

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

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 همه 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 در نظر 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 محرمانه مشتریان، فایل‌های تجاری و یا دستکاری شدن اطلاعات کلیدی سازمان همچنان بتواند پابرجا بماند؟ کشورهای درحال توسعه باید ظرفیت منابع انسانی آموزش‌دیده و زیرساختهای فناوری خود را بهبود بخشند تا اهداف آسانی برای حمله تبهکاران فضای رایانه‌ای نباشند. در این کتاب بحثهای بسیاری درباره 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 حوزه امنیت اطلاعات می‌نگرند؛ کسانی که با مکانیزمهای فنی ذخیره و ارسال اطلاعات سر و کار دارند این بحث را از دید امنیت سیستم و شبکه می‌بینند؛ حال آنکه دیگری که به تجارت مشغول هستند به آن بعنوان یک حوزه 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

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^{۱۱} 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 همدارها 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 درباره سیستمهای رایانه‌ای و امنیت شبکه است، و گروههایی که اصول اساسی را درک کرده‌اند نیز معمولاً در فهم چگونگی سازگاری 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 گرانبه بودند در نظر 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 در نتیجه کاربران و راهبران به قربانیان توسعه اطلاعات مربوط به امنیت فناوری تبدیل می‌شوند.

نقص امنیتی شبکه در همه کشورها اتفاق می‌افتد و حتی ممکن است موجب تحت فشار قرار گرفتن دولتها نیز بگردد. معمولاً بسیاری از این نقصها گزارش نمی‌شوند؛ چراکه اطلاع

خواننده باید توجه داشته باشد که مؤلفین برای مقوله امنیت و رایانه از اصطلاحات مختلفی استفاده کرده‌اند. بطور کلی مقوله 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^{۱۲}:** 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 کامیاب ترادف 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 روزمره 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.infodiv-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@infodiv-security.net ارسال نمایند.

تدوین این کتاب بدون حمایت تعدادی از افراد و مؤسسات ویژه و مهم هیچگاه ممکن نبود، از جمله سیمسون گارفینکل^{۱۳}، که راهنماییهای مهمی در تدوین ساختار اولیه این کتاب نمود و پس از آن در شناسایی و هماهنگ‌سازی قسمتی از تیم تهیه‌کنندگان کتاب کمک کرد. انتشار این

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

ما عمداً 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 به‌روزرسانی شده باشد، و دوم اینکه اطلاعات مفید و مناسبی به خوانندگانی که بدنال کسب اطلاعاتی درباره 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.

عملیاتی بانک جهانی^{۲۶} نیز تشکر نماییم. نوشته‌های وی در مورد خدمات مالی الکترونیکی^{۲۷}، تهدیدات چندوجهی^{۲۸} و مدیریت خطر سیار^{۲۹} در بخش سوم این کتاب مورد استفاده قرار گرفته‌اند.

ماکس اشلنمن^{۳۰} نماینده سوئیس در کمیته توسعه اطلاعات در اجلاس چانگ کین^{۳۱} چین در سال ۲۰۰۲ نیز یکی از اولین کسانی بود که اهمیت و فایده دستنامه 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^{۳۲} 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 نسخه نهایی این کتاب ارائه کردند؛ و ما در اینجا از راهنماییهای سازنده ایشان تشکر می‌کنیم؛ و همچنین مراتب تشکر و امتنان خود را به تمامی دست‌انکاران و افرادی که به روند چاپ این کتاب کمک کردند اعلام می‌نماییم.

این کتاب نه مرجعی آموزشی برای سیستم‌عاملهای Windows، Unix 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^{۳۳} پیشنهادی موجود اینترنت استفاده می‌کنند باید جانب احتیاط را رعایت کنند؛ چراکه ممکن است بعد از ایجاد تغییرات در هسته^{۳۴}، معماری و یا دستورات سیستمها، ارزیابی تأثیرات امنیتی آنها در سطح کلان بسادگی

کتاب راهنما بدون راهنمایی و کمک او میسر نمی‌شد. برونو لنوین^{۱۴}، مدیر infoDev که اعتبارات زیادی برای فهمیدن مناسبت و قدرت خلق اطلاعات و توزیع آن در زمینه فناوری اطلاعات و ارتباطات اختصاص داد؛ همچنین ژاکلین دوبو^{۱۵}، الی الوی^{۱۶}، تری ناکازل^{۱۷} و هریری برتادو^{۱۸} که همگی از مدیران infoDev هستند. از تیم اوریلی که با پشتیبانی شرکت خود به نام اوریلی و شرکا^{۱۹} دو کتاب زیر را منتشر کردند نیز تشکر می‌کنیم: امنیت اینترنت و کاربرد یونیکس^{۲۰}، ویرایش سوم (سیمسون گارفینکل، ژن اسپافورد^{۲۱} و آلن شوارتز^{۲۲}، چاپ ۲۰۰۳) و امنیت وب، محرمانگی و تجارت^{۲۳} (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 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 گردآوردندگان 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 نمونه همکاری تخصصی و به‌اشتراک‌گذاری اطلاعات در تمدن نوین اینترنتی امروز است.

در اینجا لازم می‌دانیم از تام کلرمن^{۲۴}، متخصص ارشد مدیریت مخاطره داده‌ها^{۲۵} در تیم امنیت خزانه بخش سیاست

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

14 Bruno Lanvin
15 Jacquelin Dubow
16 Ellie Alavi
17 Teri Nachazel
18 Heriri 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

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 شرکتی 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.