

# INFORMATION PREFACE TECHNOLOGY SECURITY

**T**he recent evolution of Information and Communication Technologies (ICTs) and the substantial innovation in the sector have resulted in a significant increase in productivity as well as the emergence of a wealth of new goods and services. As the power, capacity, and cost of microelectronics continue to improve, providing a 30% gain, approximately, in productivity and power per unit of cost each year, we have all been beneficiaries of these trends. Today we live in a digital world, where information processing is inexpensive and telecommunications costs are decreasing. It is an increasingly interconnected world.

The wealth of new technical possibilities gives rise not only to new products and more efficient and effective ways of doing things, but also to the possibility of misuse of the technology. Like other technologies, ICTs are essentially neutral, and can be used in ways that most of us would consider beneficial, as well as in ways that are harmful. The work of ICTs is done at microsecond speed, carrying information invisible to the naked eye, under the control of software developed by people, so harmful intentions in this environment are often carried out rapidly, invisibly, and are difficult, if not impossible, to trace.

The problems associated with securing information systems, the processes that depend on them, and the information that is transmitted and stored in electronic form, are not new. Major commercial systems implemented on computers have been in existence for about 50 years. The commercial banking system has been executing electronic funds transfers for about the same amount of time. In these commercial systems, there are strong incentives for criminals to attempt to compromise both solitary computers and computer networks for personal gain. In reaction to the rise in opportunities for criminal activity, significant research and development initiatives have been launched to produce stronger security measures for both information processing and communications.

In the last 50 years, much has changed. The personal computer revolution which started in the mid-1970's has put computers of remarkable size and power into the hands of hundreds of millions of people at the present time. In addition, the Internet and other forms of personal networking have enabled computer-to-computer communications among many of those people. Twenty-five years ago computing and communications were generally handled by a small group of relative experts; today hundreds of millions of people use computers for every imaginable information-processing task. They are tied together by a powerful communications network, the Internet, that allows expanded interpersonal communication via e-mail and instant messaging. The Internet also provides easy and relatively inexpensive access to a rich and growing body of digital content. Yet with these rapid technology advances, trouble spots have emerged as well. The average networked computer user of the 1970s was a professional computer specialist; today the average user is fairly ignorant, or at least is unconcerned with the technical details involved with the operations of the computer and its network. As a result, these casual users may fail to put proper security software packages and procedures in place, so that weak links in the network may be exploited by hackers or computer criminals, regardless of the respective geographical locations of the user, the exploiter, and the system being exploited.

If you use computers at home or at work, you have a certain level of responsibility for them and this publication will help you understand the procedural and technical details of managing either a single computer or a networked group of computers. Security is everyone's business, whether you are a casual user, a technician, a system administrator, a network administrator, or a manager with responsibility for systems or networks. Understanding what the central security issues are, taking prudent actions to protect your systems, and putting a set of effective security policies in place are critical steps you must take to ensure that your machines and information

will be secure from unauthorized access and that you will be able to exchange that information securely with others on the network.

This Handbook is being prepared during a time of excitement about the potential of ICTs in furthering economic and social development. While ICTs have been used for 40 years or more in many sectoral projects implemented by multilateral and bilateral aid agencies, the notion that ICTs are a critical crosscutting theme for many development initiatives is relatively new, dating back to the rise of the Internet in the early 1990s. This concept was first formalized in a multilateral agency by the infoDev Program at the World Bank Group in 1995, and was supported by the strong vision that its President, James Wolfensohn, projected on the importance of knowledge sharing for economic and social development. Since that time, optimism in the development community has run high, fed in part by the enthusiasm generated by technological developments embodied in low-cost PCs and the World Wide Web.

In 2001, the G-8 countries established the Digital Opportunity Task Force (DOT-Force). The DOT-Force presented the conclusions of its work in a report and proposed the nine-point Genoa Plan of Action, both of which were fully endorsed by G8 Leaders at their 2001 Genoa Summit. The original membership of DOT-Force includes stakeholders from the G8 and developing country governments, the private and not-for-profit sectors, and a range of international organizations.<sup>1</sup> The report presented seven action points as critical issues for creating the information society:

- 1) policy support;
- 2) improved access;
- 3) human resource development;
- 4) cultivation of entrepreneurs and entrepreneurial activity;
- 5) participation by developing countries in international conferences in IT;
- 6) IT for health; and
- 7) local content and applications

One outcome of the report was the creation of the United Nations Secretary General's ICT Task Force. Another was the creation of the Global Digital Opportunities Initiative, sponsored by UNDP, the Markle Foundation, and Accenture. Bilateral aid agencies gave increased attention to ICT in their development plans. The ITU and UNESCO made plans to host a series of two global summit meetings, the World Summit on the Information Society (WSIS), in Geneva (December 2003) and in Tunis (April 2005).<sup>2</sup>

ICTs have the potential to support, in an indirect manner, many activities aimed at achieving the Millennium Development Goals (MDGs).<sup>3</sup> Responsible IT security policies and implementation in a country will encourage the flow of foreign direct investment into that country. These flows will assist in financing the extension of a secure infrastructure that will allow ICT to contribute to these goals.

It's appropriate to ask why a publication such as this, written primarily for readers in developing countries, is needed. After all, the principles of security are the same, whether you are in a developed or a developing country. The technology is similar and the threats can come from any part of the world, no matter where you are located. A great deal of material has already been written about computer and network security and is available, although not always conveniently or cheaply, in developing countries.

First, it is important to remember that computer users and administrators in developed countries and regions have abundant access to technical and user information that assists them in their work. Bookstores and libraries are plentiful. Many technically skilled people use computers, so advice and assistance from peers is easily obtained. When computer or network problems arise, such as the spread of a virus, there is a rich set of information channels through which news and security patches are transmitted. Organizations using computers and networks have help centers staffed by technical specialists who are alert to the possibilities of misuse and make efforts to protect their organization's resources.

<sup>1</sup> About the DOT-Force, <http://www.dotforce.org/about/>, para 1.

<sup>2</sup> Information about summits, regional conferences and other events of the WSIS is available at: <http://www.itu.int/wsis/>

<sup>3</sup> See the UN Secretary General's Report on Implementation of the UN's Millennium Declaration which is available as a pdf file on the MDG website: <http://www.un.org/millenniumgoals/>

Users and technical administrators in developing countries often lack such support. The density of users is low, so anecdotal evidence that may contain warnings and solutions is lacking. Organizations using computers are often so short-staffed that they cannot afford to monitor and support their internal technical resources sufficiently. Many times, basic precautions are not taken because the underlying knowledge of computer systems and network security is insufficient. For groups that understand the basics, there may be gaps in understanding how to adapt general technical guidelines to diverse and ever-changing circumstances in the field. Vendor support, which was abundant in past years when only a few large and expensive computers were purchased, simply does not exist at the mass level at the present time. Computer stores and repair services are often unaware of problems affecting other parts of the world. As a result, users and administrators are victims of information poverty in IT security, an area where they should be well informed and up-to-date.

Failures in security occur in all countries and some breaches are made public in the press or through various electronic means. Many failures are not reported, however, in part because of embarrassment and in part because public knowledge of the failure could lead to further intrusions and unwanted results. Organizations and governments in developed countries can generally withstand some level of security failure. However, the consequences of security failures in developing countries could be considerably more serious than in the developed countries. It is our belief that businesses, organizations, and governments in developing countries do not have the same degree of resiliency to recover from such failures, because lack of awareness may lead to more massive breaches and because a malicious attack may be more catastrophic, in terms of money, reputational and psychological effects (loss of trust), and the time required to fix the problems, if they are repairable at all.

Developing countries should regard security as a top priority, for the opportunity costs of not doing so may be very high indeed. For example, criminal activity will migrate to places where controls are poor and security is weak. E-commerce and e-business activities are likely to make interesting targets in countries that are less conscious of IT security. What small or medium size business could survive an erasure of its electronic business files,

theft of its confidential customer data, or an accidental or deliberate alteration of key business information? Developing countries need to build capacity in terms of trained human resources and in terms of the technological infrastructure that will protect them from being easy targets of hackers and computer criminals.

In preparing this publication, we have had considerable discussion of what the title should be, in part because there are various views regarding what needs to be secured. Persons concerned with content tend to view this as an information security issue. Others, concerned with the technical mechanisms for storing and transmitting information, may view it as a system and network security issue. Still others may view it as an extension of e-business and think of the area as e-security.

We have chosen to think of this set of issues under the umbrella of *information technology security*. By this we mean to include all of the mechanisms for storing, processing and transmitting information including hardware, software and communications facilities, but with an equal focus upon the security of the information itself. It is important that both the information and the mechanisms that process it in any way be secure from compromise.

We have, however, intentionally limited the focus of this publication to computers, software, and networks, realizing that there is a rich set of issues in the area of fixed line and mobile telephony that have not been addressed in details here. As the convergence of telephony and computers continues, these issues are likely to become more important. With the emergence of voice over IP and ENUM, digital telephony protocols that are increasingly used, and the emergence of 3G technologies, there are clearly security issues in this space that will need to be understood and addressed.

This publication has been created so that it can be provided to the developing world without cost, thanks to a farsighted collaboration between the State Secretariat for Economic Affairs of the Government of Switzerland and the infoDev program managed by the World Bank. The goal is not only to achieve wide distribution of the hardcopy version of the publication, but also to provide its contents on a universally accessible web site. This web site will be dynamic

in two ways. First, the site's content will be updated as needed to make it current, applicable, and effective for readers in developing countries. Second, the web site will include, as appropriate, contributions from readers who provide material that assists in the evolution of the site/handbook and that offers additional guidance to those seeking information on IT security.

The following material is organized into five parts, each of which is oriented to specific groups of readers. Observant readers will notice that there is occasionally significant repetition across parts. This is intentional, since we believe that many readers will select and read only those parts that they believe are relevant to them. Some of the parts, notably the part describing security and the individual, could possibly be extracted and distributed independently to individual computer users who might well have no need of any of the other parts.

In preparing such a publication, we have had to balance the need to impart general principles with specific examples and practical information. We hope that the balance represented here is approximately correct. However, as the technology evolves and matures, the technical details are going to change. The principles, if well chosen, are likely to be invariant, so that the reader should work toward an understanding of the principles, both on the policy and management side and on the technical side. If the principles are well understood, then the technical solutions will always be discoverable for implementation.

The reader will note that the authors of the Handbook have used several different terms to refer to security and computing. In general, we have referred to **IT security**, as it can serve as an umbrella for:

- 1) **computer security**: security in a technical context: machines, software, data, and networks. The term "computer security" is commonly used in Part 2 and Part 5, as these Parts are focused on the physical, infrastructural, and technical aspects of IT security, and
- 2) **cyber-security**: IT security in a government/public policy context. The term "cyber-security" is commonly used by government agencies and public policy makers

in documents, legislation, and research projects. It is more or less synonymous with the term "**Internet security**," a term that we do not use in this Handbook, but which is sometimes used in other publications. Both terms focus on the network aspects of security and the policy implications of a networked world, including issues in privacy, crime, commerce, and global communications. The line between these terms is not sharp; as we have seen in many chapters of this Handbook, the security of your computers, networks, and data are critically intertwined with the more ephemeral concept of security in cyberspace. The term "cyber-security" appears often in Part 4.

In a fast moving technical environment, the reference material in these annexes risks becoming out of date soon after it is published. In order to make this a living document, all of its sections can be found on the web site [www.infodiv-security.net](http://www.infodiv-security.net) and each section will be updated periodically with additional useful information, with the date of last update at the bottom of each page. Readers who would like to recommend material to be used for updating the document on the web are encouraged to do so by sending suggestions via e-mail to [contact@infodiv-security.net](mailto:contact@infodiv-security.net).

This Handbook would not have been possible without the support and dedication of a number of key individuals and institutions.

Simson Garfinkel deserves special recognition for his early guidance in critiquing the initial structure of the publication. He further assisted in helping to identify and assemble part of the team to prepare the Handbook. The publication would not have been possible without his advice and assistance.

Bruno Lanvin, Manager of the *infoDev* Program of the World Bank Group, deserves substantial credit for understanding the relevance and power of knowledge creation and distribution in the field of ICT. His support in the production of this publication has been reassuring and welcome. He has been ably assisted by his colleagues Jacqueline Dubow, Ellie Alavi, Teri Nachazel and Henri Bretadeau of the *infoDev* staff.

We are extremely grateful to Tim O'Reilly, who provided access to the material contained in two important books published by his company, O'Reilly & Associates: PRACTICAL UNIX AND INTERNET SECURITY 3RD EDITION (Simson Garfinkel, Gene Spafford, and Alan Schwartz, O'Reilly & Associates, Inc. 2003) and WEB SECURITY, PRIVACY & COMMERCE (Simson Garfinkel with Gene Spafford, O'Reilly & Associates, Inc. 2002). These books were used to develop significant parts of this Handbook and a number of sections have been reprinted with permission from these authors and the publisher.

In addition, for the last ten years, O'Reilly & Associates have donated tens of thousands of technical books to people from developing countries who have attended training workshops run by the Internet Society and similar organizations. Readers who have observed the state of libraries and access to published material in the developing world will understand how significant O'Reilly's contribution is towards the ability of these countries to introduce, spread, and exploit the Internet in their countries and thereby reduce of the digital divide.

We want to warmly thank the authors of the above O'Reilly books, Simson Garfinkel, Alan Schwartz, and Gene Spafford, for their able and willing assistance in making the material in the above books suitable for use for parts of this Handbook. Their spirit of willingness to help exemplifies the best that is in the original Internet culture of professional cooperation and information sharing.

We also thank Tom Kellermann, Senior Data Risk Management Specialist in the Integrator Group and Treasury Security Team of the Operations Policy Department at The World Bank for his advice and support. His materials on e-finance, blended threats, and mobile risk management have been particularly valuable to the team and are reflected frequently in Part 3 of this Handbook.

Max Schnellmann, Switzerland's representative to the *infoDev* Donor's Committee meeting in Chongqing, China in December 2002, was among the first to realize that an IT security handbook would be extremely useful

in developing countries. His persistence in obtaining the support of the Swiss Government for the *infoDev* project to produce this Handbook was absolutely essential, and his personal support for the idea of the Handbook has carried us forward over the past year.

Michel Maechler assembled an energetic and able set of experts to review drafts of this material. Together they made many valuable suggestions that contributed to the accuracy, readability, and relevance of the final version of the publication. We are grateful for their collective experience and for their constructive guidance.

We would like to express our gratitude to all of these people for their assistance and support in preparing the first version of this document.

This Handbook is not intended to be a tutorial on Unix, Windows, or Macintosh platforms, nor is it a system administration tutorial. Use this Handbook as an adjunct to tutorials and administration guides. Managing wide-scale changes in computer systems may make them more difficult to maintain, even though the changes are needed to provide better security overall. For the convenience of the readers, we have referred to many respected online resources. However, as readers consider using programs and suggested fixes posted on the Internet, caution should be exercised. It can be challenging to evaluate the overall security impact of changes to your systems kernel, architecture, or commands. If third party patches and programs are routinely downloaded and installed to improve system security, overall security may worsen in the long term. Attention must be paid to compatibility with system requirements and the quality and reputation of the companies offering programs and advice. We hope that this Handbook will make these tasks easier and we trust that our readers will help us refine this text over time.