

EXECUTIVE SUMMARY

Information Technology Security Handbook is a practical guide to understanding and implementing IT security in your home or business environment. It has been written primarily for readers in developing countries, although the Handbook provides best practices valid in any situation. In addition to summarizing current physical and electronic threats to IT security, the Handbook also explores management practices, regulatory environments, and patterns of cooperation that exist among businesses, governments, professional associations, and international agencies today. The Handbook is structured in five Parts that may be circulated individually, though the greatest benefits will be obtained by reviewing the document in its entirety. This Executive Summary will cover the main themes of the Handbook and will offer a brief mapping of each Part in “Highlights from the Handbook.”

Adoption of ICTs Is on the Rise...

The Handbook begins with an overview of the growth of the Information Communication Technology (ICT) sector, as we know it today. This growth includes individual users of ICTs, as reflected in the rise in the number of home networks and growth in the small and medium sized enterprise sector which relies on computing resources in support of non-technical business endeavors, (restaurants or retail shops, for example) and in businesses that are tightly linked to technology development and deployment around the world (small software firms or technology outsourcing service providers, for example).

Yet Knowledge of IT Security Practices Lags Behind

While the expansion of the market for technology products and services has been dramatic at the individual and the organizational level, knowledge of IT security issues has lagged behind. Individual users may not be aware of the risks involved with surfing the Internet on their home computer. If they do recognize the dangers of unprotected networking, they may still postpone learning about firewalls, virus scanners, encryption, and regular maintenance due to the perceived financial costs, time investment,

or disruption of their current computing behavior. Small and medium sized organizations may also delay securing their systems for these reasons; in addition, they may deploy a technical solution, such as a firewall, but may not take a layered approach to security, without which their defense perimeter will still be weak. SMEs may neglect to put clear security policies and procedures in place for managers and employees to follow. If communications, awareness, and training are lacking throughout the organization, the technological defenses could be compromised quite easily through negligence before actively malicious behavior was even a factor.

Technology in a Changing Environment: Mobile Devices, Emerging Applications, and Blended Threats create complexity

New and inexperienced users are not the only cause of IT security breaches at the present time. The ICT environment is also changing rapidly with the introduction of new products, especially mobile devices (laptops, cellular phones, and Personal Digital Assistants, for example) that present different challenges to infrastructure and data security. Emerging computing applications including e-finance and e-commerce also create complexity in the networked environment. From ATM machines to online banking, these capabilities offer convenience and cost savings, but they also introduce new opportunities for theft and fraud. To make matters worse, would-be attackers are now able to develop blended threats: combinations of viruses, worms, and Trojans that may cause greater damage to systems and data than the individual forms of such “malware” can cause alone. Since all of these developments affect users of technology worldwide, the best solutions will come through international cooperation.

International Cooperation and Security in the Developing Country Context

IT security is a critically important issue for developing countries. It is well understood that the Internet offers opportunities for communications and commerce that were hardly imaginable ten years ago. Though access is not always cheap, the Internet enables users to view a tremendous variety of content and people connect via e-mail far more efficiently than they could through traditional postal services. The Internet has also affected international trade frontiers; businesses in developing countries may now offer their goods and services online – although the market may still be crowded with competitors, at least prospective customers can find information about companies, their capabilities, and their products without having deep local knowledge. While the potential for businesses to reach across geographic borders is exciting, it will take a significant amount of international cooperation to sustain the vision of a productive, globally networked world.

I. HIGHLIGHTS FROM THE HANDBOOK: IT SECURITY FOR DEVELOPING COUNTRIES

Highlights for Part 1. IT Security in the Digital Age

Part 1 of the Handbook provides an introduction to the general issues of security in an electronic age. While people have always been concerned about security issues, the advent of computers and networks has changed the terrain in a manner in subtle ways. This section describes the scope of IT security issues, explains several types of malicious behavior with respect to computers and networks, and outlines the risks of operating without adequate security measures in place.

Chapters of Part 1 include:

- The Digital Revolution
- Defining Security
- Emergence and Growth of the Internet
- Overview of Security Issues
- Perpetrators of Attacks on IT Security

Awareness of general IT security issues, including the existence and prevalence of specific security threats will help users, managers, and policy makers design effective strategies to strengthen their networks, at home and at work, against breaches.

Highlights for Part 2. IT Security for Individuals

Part 2 of the Handbook is aimed at individuals who use computing and networking resources for a variety of purposes, whether they are at home or in an office environment. This part may also be relevant for small organizations that cannot fully address IT security policy and its administration at an organizational level. It explains principal security issues for individual users and offers guidelines on techniques that will minimize the threat of a security penetration (if they are properly employed).

Some of the issues and techniques described in Part 2 include:

- why computer and network security are necessary; the impact of security breaches;
- physical security, backups, and authentication through usernames and passwords;
- the various forms of malware (malicious software) and how they spread;
- how e-mail and the Internet work and why they are a vehicle for computer attacks;
- software tools including virus checkers, firewalls and remote access tools;
- more advanced concepts such as TCP/IP networking and encryption, for the interested user.

Part 2 covers these security issues and mitigation techniques in technical detail, with the individual user in mind; Part 3 looks at security from an organizational perspective.

Highlights for Part 3. IT Security for Organizations

Part 3 of the Handbook addresses the administrative and policy aspects of security from an organizational point of view. Good security policy and its effective implementation minimize the risk of accidental and deliberate

losses, makes intrusions more difficult, and provides the tools to identify attacks and to repair security breaches. Such a combination of policy and implementation should aim to protect confidential data and help to assure the integrity of the programs and the data that are stored and transmitted over the network. This part covers the elements of effective security policy for a range of organizations, including businesses, governments, universities, and community, or non-profit organizations.

Part 3 covers the following subjects in detail:

- the eight pillar approach to security, particularly valuable in a financial services or transaction-based environment;
- security risk evaluation and loss analysis in a business context;
- policy and procedural issues to consider during the security planning process;
- the role of management in ensuring computer, network, and data security;
- personnel security: training and awareness, the hiring process, and outsourcing the security function;
- computer crime, incident reporting, and recovery;
- wireless technologies and emerging security threats to the enterprise;
- additional guidelines and checklists aimed at designing and implementing a strong organizational security practice.

Part 3 also provides an overview of public policies that are directly related to business, non-profits, and government operations in a networked world and concludes with excerpts from the World Bank's "Global Dialogues" on IT security. Part 4 contains a deeper discussion of regulatory and public policy issues in "cyberspace" and examines these issues in an international context.

Highlights for Part 4. IT Security and Government Policies

Part 4 of the Handbook addresses security issues that need to be understood and handled at the governmental level. In addition to securing its own information assets, a government has an obligation to set policy for securing the national information infrastructure; this policy has an important role to play in the promotion of IT security. There is a paradox, however: a sound public policy framework can enhance security, but ill-considered government regulation can do more harm than good. Technology is changing so rapidly and new cyber threats are emerging with such swiftness that government regulation can become a straitjacket, impeding the development and deployment of innovative responses. It is important therefore to achieve the right balance of regulatory and non-regulatory measures. Clearly, government cyber-security policies must take into account the technical and social characteristics of the Internet. Within this context, governments can take a range of steps to improve computer security, without interfering with technical design decisions.⁴

Part 4 contains an in-depth discussion of the following subjects:

- the communications network and other critical infrastructures that are owned and operated by the private sector, but regulated by the government; a picture of mutual dependency;
- the government's general role and responsibilities in promoting sound computer security practices in the public, private, and non-profit sectors;
- computer crime laws that must protect both government and privately-owned computers and networks;
- traditional concepts of legal liability translated to the computer context;
- laws, regulations, and government policies that are focused on promoting computer security in areas of consumer protection, data and communications privacy, and frameworks for e-commerce; and

⁴ The following discussion draws upon the detailed surveys compiled by the American Bar Association's Privacy & Computer Crime Committee: Jody R. Westby, ed., *International Guide to Combating Cybercrime*, American Bar Association, Section of Science & Technology Law, Privacy & Computer Crime Committee, 2003, <http://www.abanet.org/abapubs/books/cybercrime/>; Jody R. Westby, ed., *International Strategy for Cyberspace Security*, American Bar Association, Section of Science & Technology Law, Privacy & Computer Crime Committee, 2003. See also *International Critical Information Infrastructure Protection Handbook*, edited by Andreas Wenger, Jan Metzger and Myriam Dunn, Center for Security Studies and Conflict Research, Swiss Federal Institute of Technology (2002) <http://www.isn.ethz.ch/crn>.

- legal and policy models from a number of countries and references to resources in relevant international organizations.

Part 4 evaluates security from legal and public policy perspectives. Part 5 takes a deeper look at the technical means and procedures required to secure IT resources.

Highlights for Part 5. IT Security for Technical Administrators

Part 5 is aimed at helping system and network administrators perform their duties efficiently. It covers security issues that need to be understood and addressed at a technical and managerial level, with examples of how security breaches occur and advice on how preventive measures may be taken. Other parts of the Handbook covered an overview of the current computing environment, security for the individual user, security from an organizational standpoint, and the legal and public policy implications of security risks and prevention. Part 5 explains in greater detail the specific threats to security, including the various methods of attack that are used to penetrate systems and program, the methods of monitoring critical systems and network traffic so that attempted intrusions can be detected, the best practices in securing such systems, and the appropriate way to handle a security incident when a breach has occurred.

Part 5 handles the following issues, with the systems administrator in mind:

- the design of secure systems and the methods of system attackers;
- the varied threats to IT security from environmental factors to vandalism, sabotage, and theft, with suggestions on how to address these threats;
- the mechanisms for protecting information from unwanted exposure, tampering, or destruction, known as *confidentiality* (preventing unauthorized users from accessing or modifying data and programs) and *integrity* (insuring that information and software remain intact and correct);
- procedures for handling users: *identification*, *authentication*, and *authorization*;
- common security problems that affect computers

being used to offer information services (servers) and how to build servers that minimizes these problems;

- network security from the hardware side (modems, routers, and wireless access) to the software side (TCP/IP, the dominant networking protocol on local area networks and the Internet);
- the techniques that are used to attack workstations and servers, namely *denial of service* attacks, *programmed threats*, and *social engineering*;
- how to use auditing, logging, and forensics to help detect compromises and identify what's been modified on a compromised system; and finally,
- technical recommendations that are specific to Unix/Linux, Microsoft Windows, and MacOS 7-9 operating systems, MacOS X is covered by the Unix material.

Due to the volume and complexity of the material, several annexes have been provided. **Annex 1** contains a Glossary of terms commonly used in information technology and communication. **Annexes 2-5** contain a bibliography of references to security resources. These sources include print resources, electronic resources, and a listing of organizations that focus on security issues. All readers of the Handbook are encouraged to learn more about specific topics by referencing the items in the bibliography.

II. FUTURE STEPS AND CONCLUSIONS

Digital technology provides us with exciting new tools that can have a major impact on education, health, commerce, and other sectors of civil society. This technology benefits all countries and peoples, but may have a special attraction for developing countries in that it can help to accelerate their integration into the world economic community. The stakes are high for these countries. Foreign direct investment, confidence, and trust in a developing country depend upon a secure and effective implementation of technology and infrastructure. Governments, organizations, and individuals all have a part to play in assuring the security of the country's electronic and information assets.

This Handbook contains a set of current best practices in security that may assist the reader in implementing the policies and procedures that are relevant to his or her situation. In addition, it includes ample references to other materials, both electronic and print, that cover specific aspects of IT security. This Handbook is one step in assisting with knowledge transfer and capacity building at the local level in the developing world. To this end, the IT Security Handbook will be offered by The World Bank as a print publication, a CD ROM, and a website which will be updated with fresh material on a regular basis. This first edition of the Handbook will be presented at the WSIS Conference in Geneva, Switzerland in December 2003.

The World Bank enjoys copyright protection under protocol 2 of the Universal Copyright Convention. This material may nonetheless be copied for research, educational, or scholarly purposes only in member countries of the World Bank that are considered to be developing countries. The findings, interpretations, and conclusions expressed in this document are entirely those of the authors and should not be attributed to the World Bank, to its affiliated organizations, or to the members of its Board of Directors or the countries they represent.

The IT Security Handbook is a living document and all of its sections can be found on the web site: <http://www.infodev-security.net>. Each section will be updated periodically with additional information on global IT security issues. Readers who would like to recommend material for publication in these updates are encouraged to send suggestions via e-mail to contact@infodev-security.net.