



IEEE Standard for Information Technology: Hardcopy Device and System Security

IEEE Computer Society

Sponsored by the
Information Assurance Committee

2600TM

IEEE
3 Park Avenue
New York, NY 10016-5997, USA
30 June 2008

IEEE Std 2600TM-2008

IEEE Standard for Information Technology: Hardcopy Device and System Security

Sponsor

Information Assurance Committee
of the
IEEE Computer Society

Approved 27 March 2008
IEEE-SA Standards Board

The following companies have agreed to make financial contributions to underwrite the cost of Common Criteria certification of some or all of the IEEE Std 2600-series Protection Profiles:

Canon Inc.; Fuji Xerox; The Hewlett-Packard Company; InfoPrint Solutions Company; Konica Minolta; Kyocera Mita Corporation; Lexmark International, Inc.; Océ; Oki Printing Solutions; Ricoh Company, Ltd.; Samsung Electronics Co., Ltd.; Sharp Corporation; Toshiba TEC Corporation; Xerox Corporation

Abstract: This standard defines security requirements (all aspects of security including but not limited to authentication, authorization, privacy, integrity, device management, physical security, and information security) for manufacturers, users, and others on the selection, installation, configuration, and usage of hardcopy devices (HCDs) and systems, including printers, copiers, and multifunction devices (MFDs), and the computer systems that support these devices. This standard identifies security exposures for these HCDs and systems, and instructs manufacturers and software developers on appropriate security capabilities to include in their devices and systems, and instructs users on appropriate ways to use these security capabilities.

Keywords: all-in-one, copier, facsimile, fax, hardcopy device, HCD, information security, MFD, MFP, multifunction device, multifunction product, printer, scanner

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

Copyright © 2008 by the Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 30 June 2008. Printed in the United States of America.

IEEE is a registered trademark in the U.S. Patent & Trademark Office, owned by the Institute of Electrical and Electronics Engineers, Incorporated.

Bluetooth is a registered trademark owned by the Bluetooth SIG, Inc.

CERT is registered in the U.S. Patent Office and Trademark Office by Carnegie Mellon University.

The EMV™ Mark is a trademark exclusively owned by EMVCo LLC.

FireWire is a registered trademark of Apple Inc.

HomePNA is a trademark of the HomePNA Alliance.

IrDA is a registered trademark of Infrared Data Association®.

Java and Java Card are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

Linux® is a registered trademark of Linus Torvalds in the U.S. and other countries.

MasterCard is a registered trademark of MasterCard Worldwide.

OCTAVE and Operationally Critical Threat, Asset, and Vulnerability Evaluation are trademarks and servicemarks owned by Carnegie Mellon University.

UNIX is a registered trademark of the The Open Group.

VISA is a registered trademark of Visa International Service Association.

Wi-Fi, WPA, and WPA2 are trademarks of the Wi-Fi Alliance.

PDF: ISBN 978-0-7381-5750-4 STD95801
Print: ISBN 978-0-7381-5751-1 STDPD95801

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher.

IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE-SA) Standards Board. The IEEE develops its standards through a consensus development process, approved by the American National Standards Institute, which brings together volunteers representing varied viewpoints and interests to achieve the final product. Volunteers are not necessarily members of the Institute and serve without compensation. While the IEEE administers the process and establishes rules to promote fairness in the consensus development process, the IEEE does not independently evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained in its standards.

Use of an IEEE Standard is wholly voluntary. The IEEE disclaims liability for any personal injury, property or other damage, of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, or reliance upon this, or any other IEEE Standard document.

The IEEE does not warrant or represent the accuracy or content of the material contained herein, and expressly disclaims any express or implied warranty, including any implied warranty of merchantability or fitness for a specific purpose, or that the use of the material contained herein is free from patent infringement. IEEE Standards documents are supplied “**AS IS**.”

The existence of an IEEE Standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE Standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard. Every IEEE Standard is subjected to review at least every five years for revision or reaffirmation. When a document is more than five years old and has not been reaffirmed, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE Standard.

In publishing and making this document available, the IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity. Nor is the IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing this, and any other IEEE Standards document, should rely upon his or her independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of a given IEEE standard.

Interpretations: Occasionally questions may arise regarding the meaning of portions of standards as they relate to specific applications. When the need for interpretations is brought to the attention of IEEE, the Institute will initiate action to prepare appropriate responses. Since IEEE Standards represent a consensus of concerned interests, it is important to ensure that any interpretation has also received the concurrence of a balance of interests. For this reason, IEEE and the members of its societies and Standards Coordinating Committees are not able to provide an instant response to interpretation requests except in those cases where the matter has previously received formal consideration. A statement, written or oral, that is not processed in accordance with the IEEE-SA Standards Board Operations Manual shall not be considered the official position of IEEE or any of its committees and shall not be considered to be, nor be relied upon as, a formal interpretation of the IEEE. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that his or her views should be considered the personal views of that individual rather than the formal position, explanation, or interpretation of the IEEE.

Comments for revision of IEEE Standards are welcome from any interested party, regardless of membership affiliation with IEEE. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Comments on standards and requests for interpretations should be submitted to the following address:

Secretary, IEEE-SA Standards Board
445 Hoes Lane
Piscataway, NJ 08854
USA

Authorization to photocopy portions of any individual standard for internal or personal use is granted by The Institute of Electrical and Electronics Engineers, Inc., provided that the appropriate fee is paid to Copyright Clearance Center. To arrange for payment of licensing fee, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Introduction

This introduction is not part of IEEE Std 2600-2008, IEEE Standard for Information Technology: Hardcopy Device and System Security.

This standard defines the security requirements and guidance for manufacturers, information technology (IT) professionals, users, and others on the selection, installation, configuration, and usage of secure hardcopy devices (HCDs) and systems. The standard defines unique security requirements for HCDs in four different usage environments that map to most HCD installations.

This standard is part of a family of standards that are related to HCD and system security. IEEE P2600.1™ [B34],^a IEEE P2600.2™ [B35], IEEE P2600.3™ [B36], and IEEE P2600.4™ [B37] provide Common Criteria protection profiles that can be used by manufacturers to create Common Criteria version 3.1 conformant Security Target documents for use in the Common Criteria certification program. Respectively, IEEE P2600.1, IEEE P2600.2, IEEE P2600.3, and IEEE P2600.4 are protection profiles that correspond to Operational Environments A, B, C, and D, as defined in this standard. The requirements for each environment listed in the compliance clause in this standard map directly to the required security objectives in the profile documents. This standard also defines additional security guidance and recommendations for non-IT security techniques that are beyond the scope of Common Criteria certification and for IT security techniques that cannot be exhaustively tested and verified in the Common Criteria certification program.

Notice to users

Laws and regulations

Users of these documents should consult all applicable laws and regulations. Compliance with the provisions of this standard does not imply compliance to any applicable regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

Copyrights

This document is copyrighted by the IEEE. It is made available for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making this document available for use and adoption by public authorities and private users, the IEEE does not waive any rights in copyright to this document.

Updating of IEEE documents

Users of IEEE standards should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect. In order to determine

^a The numbers in brackets correspond to those of the bibliography in Annex B.

whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit the IEEE Standards Association Web site at <http://ieeexplore.ieee.org/xpl/standards.jsp>, or contact the IEEE at the address listed previously.

For more information about the IEEE Standards Association or the IEEE standards development process, visit the IEEE-SA Web site at <http://standards.ieee.org>.

Errata

Errata, if any, for this and all other standards can be accessed at the following URL: <http://standards.ieee.org/reading/ieee/updates/errata/index.html>. Users are encouraged to check this URL for errata periodically.

Interpretations

Current interpretations can be accessed at the following URL: <http://standards.ieee.org/reading/ieee/interp/index.html>.

Patents

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken with respect to the existence or validity of any patent rights in connection therewith. A patent holder or patent applicant has filed a statement of assurance that it will grant licenses under these rights without compensation or under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination to applicants desiring to obtain such licenses. Other Essential Patent Claims may exist for which a statement of assurance has not been received. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims, or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

Participants

At the time this standard was submitted to the IEEE-SA Standards Board for approval, the P2600 Standard Working Group had the following membership:

Don Wright, *Chair*
Lee Farrell, *Vice Chair*
Brian Smithson, *Secretary*
Jerry Thrasher, *Editor*

Hiromasa Akamatsu
Carmen Aubry
Ron Bergman
Shah Bhatti
Nancy Chen
Peter Cybuck
Nick Del Re
David Freas
Fusayuki Fujita
Satoshi Fujitani
Tom Haapanen
Kazutaka Higo

Hiroshi Hosaka
Akihiko Iwasaki
Harry Lewis
Jean-Claude Longo
Daniel Manchala
Takanori Masui
Takeshi Nakamura
Ron Nevo
Wanda Nuckolls
Yusuke Ohta
Ken Ota
Glen Petrie

Stuart Rowley
Ole Skov
Alan Sukert
Yasuji Takeuchi
Hiroki Uchiyama
Shigeru Ueda
Brian Volkoff
Bill Wagner
Jan Walter
Craig Whittle
Sameer Yami
Liang Zhao

The following members of the individual balloting committee voted on this standard. Balloters may have voted for approval, disapproval, or abstention.

Danilo Antonelli
Carmen Aubry
Matthew Ball
Massimo Cardaci
Juan Carreon
Ying Chen
Keith Chow
John Cole
Geoffrey Darnton
Russell Dietz

Lee Farrell
Randall Groves
Tom Haapanen
Mark Henley
Eric Hibbard
Werner Hoelzl
Raj Jain
Piotr Karocki
Michael S. Newman

Charles K. Ngethe
Michael D. Rush
Brian Smithson
Thomas Starai
Walter Struppler
Jerry Thrasher
Thomas Tullia
Paul Work
Don Wright
Sameer Yami

When the IEEE-SA Standards Board approved this standard on 27 March 2008, it had the following membership:

Robert M. Grow, *Chair*
Thomas Prevost, *Vice Chair*
Steve M. Mills, *Past Chair*
Judith Gorman, *Secretary*

Victor Berman
Richard DeBlasio
Andy Drozd
Mark Epstein
Alexander Gelman
William R. Goldbach
Arnold M. Greenspan
Kenneth S. Hanus

Jim Hughes
Richard H. Hulett
Young Kyun Kim
Joseph L. Koepfinger*
John Kulick
David J. Law
Glenn Parsons

Ronald C. Petersen
Chuck Powers
Narayanan Ramachandran
Jon Walter Rosdahl
Anne-Marie Sahazizian
Malcolm V. Thaden
Howard L. Wolfman
Don Wright

*Member Emeritus

Also included are the following nonvoting IEEE-SA Standards Board liaisons:

Satish K. Aggarwal, *NRC Representative*
Michael H. Kelley, *NIST Representative*

Jennie Steinhagen
IEEE Standards Program Manager, Document Development

Michael D. Kipness
IEEE Standards Program Manager, Technical Program Development

Contents

1. Overview	1
1.1 Scope	1
1.2 Purpose	1
1.3 Document structure.....	2
2. Definitions, special terms, acronyms, and abbreviations.....	3
2.1 Definitions	3
2.2 Special terms.....	3
2.3 Acronyms and abbreviations	7
3. Introduction to hardcopy devices	13
3.1 Hardcopy device overview	13
3.2 Generic architecture.....	13
3.3 Similarities and differences between HCDs and other IT devices.....	16
3.4 Determining the appropriate security strategy for an HCD	18
4. Operational environments.....	21
4.1 Background.....	21
4.2 Operational Environment A.....	21
4.3 Operational Environment B	26
4.4 Operational Environment C	31
4.5 Operational Environment D.....	33
4.6 Choosing the most applicable operational environment	36
5. Hardcopy device assets.....	38
5.1 Overview	38
5.2 HCD asset definitions.....	38
5.3 Asset values in the operational environments.....	39
6. Hardcopy device threats	41
6.1 Overview	41
6.2 Threat summaries	41
6.3 Threat vectors and descriptions	44
6.4 Threat risk levels	69
7. Threat mitigation techniques	71
7.1 Mitigating threats to HCD Availability	71
7.2 Mitigating threats to HCD Physical Resources	83
7.3 Mitigating threats to HCD User Document and User Function Data	86
7.4 Mitigating threats to HCD Confidential and Protected Data	103
7.5 Mitigating threats to HCD software.....	112
7.6 Mitigating threats to the HCD External Environment	114
8. Compliance.....	117
8.1 Compliance security objectives for HCD manufacturers.....	117
8.2 Compliance security objectives for IT professionals.....	128
Annex A (informative) Best practices	136
Annex B (informative) Bibliography.....	171

IEEE Standard for Information Technology: Hardcopy Device and System Security

IMPORTANT NOTICE: *This standard is not intended to assure safety, security, health, or environmental protection in all circumstances. Implementers of the standard are responsible for determining appropriate safety, security, environmental, and health practices or regulatory requirements.*

This IEEE document is made available for use subject to important notices and legal disclaimers. These notices and disclaimers appear in all publications containing this document and may be found under the heading “Important Notice” or “Important Notices and Disclaimers Concerning IEEE Documents.” They can also be obtained on request from IEEE or viewed at <http://standards.ieee.org/IPR/disclaimers.html>.

1. Overview

1.1 Scope

This standard defines security requirements (all aspects of security including but not limited to authentication, authorization, privacy, integrity, device management, physical security and information security) for manufacturers, users, and others on the selection, installation, configuration and usage of hardcopy devices (HCDs) and systems; including printers, copiers, and multifunction devices (MFDs). This standard identifies security exposures for these HCDs and systems, and instructs manufacturers and software developers on appropriate security capabilities to include in their devices and systems, and instructs users on appropriate ways to use these security capabilities.

1.2 Purpose

In today’s information technology (IT) environment, significant time and effort are being spent on security for workstations and servers. However, today’s HCDs (printers, copiers, MFDs, etc.) are connected to the same local area networks (LANs) and contain many of the same communications, processing and storage components, and are subject to many of the same security problems as workstations and servers. At this time, there are no standards to guide manufacturers or users of HCDs in the secure installation, configuration, or usage of these devices and systems.

The purpose of this document is to serve as such a standard and its goals are:

- a) To provide guidance in the secure architecture, design, and out-of-box configuration of HCDs for manufacturers;
- b) To provide guidance in the secure installation, configuration, and use of HCDs for end users and their supporting organizations.

1.3 Document structure

Clause 1 provides the scope and purpose of the standard and an overview of the standard's structure.

Clause 2 provides the definitions, special terms, acronyms, and abbreviations used in this standard.

Clause 3 describes the structure, architecture, and functions of a hardcopy device.

Clause 4 describes the various security environments of hardcopy devices considered by this standard.

Clause 5 describes the various assets of an HCD.

Clause 6 describes the threats against HCDs that are considered by this standard.

Clause 7 describes some of the mitigation techniques used to address each threat described in Clause 6. Mitigation techniques are provided for manufacturers, IT administrators, and users.

Clause 8 indicates specific security objectives, by operational environment, that are mandatory for compliance with this standard and provides example mitigation techniques that may be used to accomplish these objectives.

Annex A describes the best practices for various general security measures for HCDs. Best practices are provided for manufacturers, IT administrators, and users of HCDs.

Annex B provides additional references, which may add to the understanding of other parts of this document.

2. Definitions, special terms, acronyms, and abbreviations

2.1 Definitions

For the purposes of this document, the following terms and definitions apply. *The Authoritative Dictionary of IEEE Standards Terms* [B38]¹ should be referenced for terms not defined in this clause.

2.1.1 hardcopy device (HCD): A system producing or utilizing a physical embodiment of an electronic document or image. These systems include printers, scanners, fax machines, digital copiers, multifunction peripherals (MFPs), multifunction devices (MFDs), *all-in-ones*, and other similar products. *See also:* **multifunction device.**

2.1.2 multifunction device (MFD): An HCD that fulfills multiple purposes by using multiple functions in different combinations to replace several, single function devices.

2.2 Special terms

Terms used in this standard are defined as follows:

access control: Security service that controls the use of hardware and software resources and the disclosure and modification of stored or communicated data.

accountability: Property that allows activities in an IT system to be traced to the entity responsible for the activity.

actor: A role that a user plays with respect to an HCD.

administrator: A user who has been specifically granted the authority to manage some portion or all of the HCD and whose actions may affect the security policy. Administrators may possess special privileges that provide capabilities to override portions of the security policy.

applet: A program designed to be executed from within another program, e.g., a Java™ virtual machine program.² Applets cannot be executed directly from the operating system (OS).

application: The software or firmware that performs a major function of the HCD, e.g., authentication, copying, printing, scanning, and facsimile (fax).

asset: An entity upon which the owner, user, or manager of the device places value.

assurance: A measure of confidence that the security features of an IT system are sufficient to enforce its security policy.

attack: An intentional act attempting to violate the security policy of an IT system.

auditor: A user who reviews and maintains the audit trail recorded by the HCD.

¹ The numbers in brackets correspond to those of the bibliography in Annex B.

² Java is a trademark of Sun Microsystems, Inc. in the United States and other countries. This information is given for the convenience of users of this standard and does not constitute an endorsement by the IEEE of these products. Equivalent products may be used if they can be shown to lead to the same results.

authentication data: Information used to verify a claimed identity.

authorized administrator: A user who has been specifically granted permission by an entity authorized to do so to manage some portion or all of the HCD and whose actions may affect the security policy.

authorized user: An authenticated user who may, in accordance with the HCD's security policy, perform an operation.

back channel: Typically a low-speed or less-than-optimal transmission channel flowing opposite to the forward channel's direction. In many cases, the back channel is used mostly for acknowledgements of the validity of the forward channel's data (i.e., that the forward channel's data passes validity tests of some sort). *Contrast:* **forward channel.**

black list: A list of specific user credential values (e.g., login ID, e-mail addresses, phone numbers, URLs) that are explicitly prohibited from accessing all or specified functions of an HCD. *Contrast:* **white list.**

compromise: Type of incident where information is disclosed to unauthorized individuals or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosures, modification, destruction, or loss of an object may have occurred.

copy control device: An entity external to the HCD, comprising hardware or software that enables and tracks copying.

copy control interface: An interface for connecting a copy control device to an HCD.

credential: A form of authentication data that specifies basic identifying information about a user or application. Credentials may be bound in some way to the individual to whom they were issued, or they may be bearer credentials. The former are necessary for identification, while the latter may be acceptable for some forms of authorization.

customer engineer: A person authorized to maintain an HCD at a customer site.

data: A representation of facts, concepts, or instructions in a manner suitable for communication, interpretation, or processing by humans or by automatic means

data interface: Any interface that transports print or scan data into or out of the HCD.

demilitarized zone (DMZ): A computer or small subnetwork that sits between a trusted internal network, such as a corporate private LAN, and an untrusted external network, such as the public Internet.

defense in depth: A security design strategy whereby layers of protection are utilized to establish an acceptable security posture for an IT system.

denial of service (DoS): The prevention of authorized access to a system resource or the delaying of system operations and functions.

device administrator: A user who controls administrative operations of the HCD other than its network configuration (e.g., management of users and resources of the HCD).

device interface: An electrical interface for connecting a device to control access to local operation of the HCD. Depending on the device and its purpose, access may be granted as a result of identifying the user or as a result of a payment. *See also:* **copy control interface.**

dictionary attack: An attack that tries all of the phrases or words in a dictionary, trying to crack a password or key. A dictionary attack uses a predefined list of words compared to a brute force attack that tries all possible combinations.

entity: A subject, object, user, or another IT device, which interacts with HCD objects, data, or resources.

external device interface: *See:* **device interface.**

firewall: A gateway that limits access between networks in accordance with local security policy.

firmware: Persistent computer instructions and data embedded in the HCD that provides basic functions of that device. Firmware is only replaced during a specialized update process.

forward channel: Communications channel used for the delivery of document data. *Contrast:* **back channel.**

identity: A representation (e.g., a string) uniquely identifying an authorized user, which can either be the full or abbreviated name of that user or a pseudonym.

information assurance: Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

information technology (IT): The hardware, firmware, and software used as part of a system to collect, create, communicate, compute, disseminate, process, store, or control data or information.

local interface: An electrical, optical, or electromagnetic (EM) interface intended for use with close physical proximity (typically no more than 10 m) to the HCD. Examples include USB [B148], FireWire® (IEEE Std 1394™-1995 [B44]), IrDA®, parallel port (IEEE Std 1284™-2000 [B43]), serial port (e.g., EIA-232-1987 [B19]), memory card, diskette, and Bluetooth® (IEEE Std 802.15.1™-2005 [B42]).³

maintenance port: An electrical interface used for machine maintenance, service troubleshooting, or firmware updates.

man-in-the-middle attack: An active attack whereby a third party attempts to surreptitiously intercept, read, or alter information moving between two computing devices or users.

media: Objects on which data are or can be imaged. These include paper, transparencies, T-shirt transfers, etc.

network administrator: A user who manages the network configuration of the HCD.

network interface: An interface used to connect the HCD to a network. Examples include IEEE 802.3™, IEEE 802.5™, and IEEE 802.11™ interfaces.

non-repudiation: (A) The prevention of false denial of involvement in sending or receiving information. **(B)** A security policy pertaining to providing one or more of the following: to the sender of data, proof of delivery to the intended recipient; to the recipient of data, proof of the identity of the user who sent the data.

³ FireWire is a registered trademark of Apple Inc. IrDA is a registered trademark of Infrared Data Association. Bluetooth is a registered trademark owned by the Bluetooth SIG, Inc. [B9]. This information is given for the convenience of users of this standard and does not constitute an endorsement by the IEEE of these products. Equivalent products may be useful if they can be shown to lead to the same results.

operational environment: The total environment in which an HCD operates, including the consideration of the value of assets and controls for operational accountability, physical security, and personnel.

operator panel: A local human interface used to operate the HCD. It typically consists of a keypad, keyboard, or other controls, and a display device.

password cracking: The process of attempting to ascertain secret passwords, often through algorithmic, dictionary, or automated procedures.

risk assessment: Assessment of threats to, impacts on, and vulnerabilities of information and information processing facilities and equipment including consideration of the likelihood of occurrence.

security objective: A statement of intent to counter identified threats or satisfy identified organization security policies or assumptions.

sniffing: Network wiretapping; passively monitoring and recording data that is flowing between two or more points in a communication system.

social engineering: Non-technical or low-technology means—such as deception, impersonation, tricks, bribes, blackmail, and threats—used to attack information systems.

spam: Unsolicited and unwanted electronic mail, instant messages, or other electronic communications.

stored data: Fonts, forms, and document data.

temporary data: The data, e.g., images, print file, that are temporarily buffered or stored in memory before or while the HCD performs application operations.

threat: Capabilities, intentions and attack methods of adversaries, or any circumstance or event, with the potential to violate the HCD's security policy.

threat agent: Any human user or IT product or system that may attempt to violate the HCD's security policy and perform an unauthorized operation with the HCD.

unauthorized user: A user who is not permitted to access or use an HCD for a defined purpose.

user: An entity (human user or IT entity) outside the HCD that interacts with the HCD.

User Document Data: The asset that consists of the information contained in a user's document. This includes the original document itself in either hardcopy or electronic form, image data, or residually stored data created by the HCD while processing an original document and printed hardcopy output.

User Function Data: The asset that consists of the information about a user's document or job to be processed by the HCD.

vulnerability: A weakness that can be exploited to violate the HCD's security policy.

white list: A list of specific user credential values (e.g., login ID, e-mail addresses, phone numbers, URLs) that are explicitly allowed access to all or specified functions of an HCD. *Contrast:* **black list.**

2.3 Acronyms and abbreviations

Abbreviations and acronyms used in this document are defined as follows:

3DES	“Triple DES” data encryption standard used three times
ADPU	active directory password utility
AES	advanced encryption standard
ANSI	American National Standards Institute
APOP	authenticated post office protocol
ASIS	American Society for Industrial Security
ATM	automated teller machine
BioAPI	Biometric Application Programmer Interface
CBC	cipher block chaining
CBEFF	common biometric exchange file format
CEN	European Committee for Standardization
CF	compact flash
CIFS	common Internet file system
CM	configuration management
COTS	commercial, off-the-shelf
CPU	central processing unit
CRC	cyclic redundancy check
C-SET	card secured electronic transactions
CSMA/CD	carrier sense multiple access/collision detection
CSN	card serial number (for compact flash)
DES	data encryption standard
DHS	U.S. Department of Homeland Security
DMZ	demilitarized zone
DoD	U.S. Department of Defense
DOE	U.S. Department of Energy

DoS	denial of service
DRAM	dynamic random access memory
DSA	directory service agent
DSL	digital subscriber loop
DSS	digital signature standard
EEPROM	electrically erasable programmable read-only memory
EIA	Electronic Industries Association
EM	electromagnetic
EMI	electromagnetic interference
EMSEC	emission security
EMV™	Europay-Mastercard®-Visa® ⁴
EN	ISO language code for English, all dialects
EPROM	erasable programmable read-only memory
ESMTP	extended simple mail transfer protocol
ESP	encapsulating security payload
ETSI	European Telecommunications Standards Institute
EU	European Union
fax	facsimile
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act of 2002 [B22]
FX	foreign exchange
GOST	<u>G</u> Oсударstvennyi <u>S</u> Tandard (Russian for “government standard”)
GSM	global system for mobile communications
HCD	hardcopy device
HDD	hard disk drive

⁴ The EMV™ Mark is a trademark exclusively owned by EMVCo LLC. MasterCard is a registered trademark of MasterCard Worldwide. The Visa trademark is owned by Visa Inc. This information is given for the convenience of users of this standard and does not constitute an endorsement by the IEEE of these products. Equivalent products may be used if they can be shown to lead to the same result.

HIPAA	Health Insurance Portability and Accountability Act
HMAC	keyed-hash message authentication code
HMG	Her/His Majesty's government
HPNA	Home Phoneline Networking Alliance
HTTPS	hypertext transfer protocol (secure)
I/O	input/output
IBIA	International Biometric Industry Association
ICC	integrated circuit card
ICMP	Internet control message protocol
ID	identification
IEC	International Electrotechnical Commission
IFD	interface device
IKE	Internet key exchange
INCITS	InterNational Committee for Information Technology Standards (USTAG to JTC1)
IP	Internet protocol version 4
IPP	Internet printing protocol
IPsec	Internet protocol security
IPv6	Internet protocol version 6
IrDA	Infrared Data Association
ISAKMP	Internet security association and key management protocol
ISO	International Organization for Standardization
ISP	Internet service provider
IT	information technology
ITL	information technology laboratory
kb/s	kilobits per second
KDC	key distribution center
LAN	local area network
LCD	liquid crystal display

LDAPS	lightweight directory access protocol (secure)
MAC	media access control
MD5	message-digest algorithm 5
METI	Japanese Ministry of Economy, Trade and Industry
MFD	multifunction device
MFM	modified frequency modulation
MFP	multifunction product/peripheral/printer
MIC	message integrity code
MICR	magnetic ink character recognition
NATO	North Atlantic Treaty Organization
NAVSO	Navy Staff Office
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
OCR	optical character recognition
OCTAVE [®]	Operationally Critical Threat, Asset, and Vulnerability Evaluation ^{SM 5}
OS	operating system
OTS	off-the-shelf
PC	personal computer
PC/SC	proximity card/smart card
PDA	personal digital assistant
PDL	page description language
PHIPA	Personal Health Information Protection Act
PIN	personal identification number
PNA	Phoneline Networking Alliance
PSTN	public switched telephone network
RADIUS	remote authentication dial-in user service

⁵ OCTAVE and Operationally Critical Threat, Asset, and Vulnerability Evaluation are trademarks and servicemarks owned by Carnegie Mellon University. This information is given for the convenience of users of this standard and does not constitute an endorsement by the IEEE of these products. Equivalent products may be used if they can be shown to lead to the same result.

RAM	random access memory
RFC	request for comment
RIP	raster image processor
RLL	run length limited
ROM	read-only memory
S/MIME	secure/multipurpose Internet mail extensions
SANS	sysadmin, audit, network, security
SCADA	supervisory control and data acquisition
SCQL	structured card query language
SCSI	small computer system interface
SEIS	secure electronic information in society
SET	secure electronic transactions
SHA	secure hash algorithm
SIM	subscriber identity module
SMI	shared media interface
SMTP	simple mail transport protocol
SNMP	simple network management protocol
SOHO	small office/home office
SRAM	static random access memory
SSH	secure shell
SSL	secure sockets layer
STANAG	standardization agreement
TACACS	terminal access controller access control system
TCP	transmission control protocol
TE	terminal equipment
TLS	transport layer security
TWIC	transportation worker identification credential
UDP	user datagram protocol

USB	Universal Serial Bus
USENIX	Advanced Computing Systems Association
USM	user-based security model
VLAN	virtual local area network
VPN	virtual private network
VSITR	Verschluss-sachen-IT-Richtlinien
WAN	wide area network
WEP	wired equivalent privacy
WPA2™	Wi-Fi® protected access 2 (an enhanced version of WPA™) ⁶
WPA	Wi-Fi protected access

⁶ Wi-Fi, WPA, and WPA2 are trademarks of the Wi-Fi Alliance [B151]. This information is given for the convenience of users of this standard and does not constitute an endorsement by the IEEE of these products. Equivalent products may be useful if they can be shown to lead to the same results.

3. Introduction to hardcopy devices

3.1 Hardcopy device overview

The HCDs that are considered in this standard are used for the purpose of converting hardcopy documents into digital form (scanning), converting digital documents into hardcopy form (printing), transmitting or receiving documents over telephone lines [public switched telephone network (PSTN) faxing], or duplicating hardcopy documents (copying). Typically, hardcopy documents are in paper form, but they can also take other forms (e.g., positive or negative transparencies or film).

HCDs can be implemented in many different configurations, depending on their intended purpose or purposes. Simple devices have a single purpose implemented by a single function, such as a printer or scanner. Other devices have a single purpose implemented by a compound function, such as a copier or fax machine. Complex MFDs fulfill multiple purposes by using multiple functions in different combinations to replace several, single function devices.

For the purposes of this standard, a generic MFD will be used as an example because it is composed of all of the individual purposes and functions of other HCDs; however, this standard can be applied to an HCD that is composed of any combination of these purposes and functions.

3.2 Generic architecture

HCD architecture and organization of functions vary widely depending upon specific functions, features, manufacturers, and other factors. For the purpose of illustration, a generic, composite architecture is shown in Figure 1, and its component parts are described subsequently.

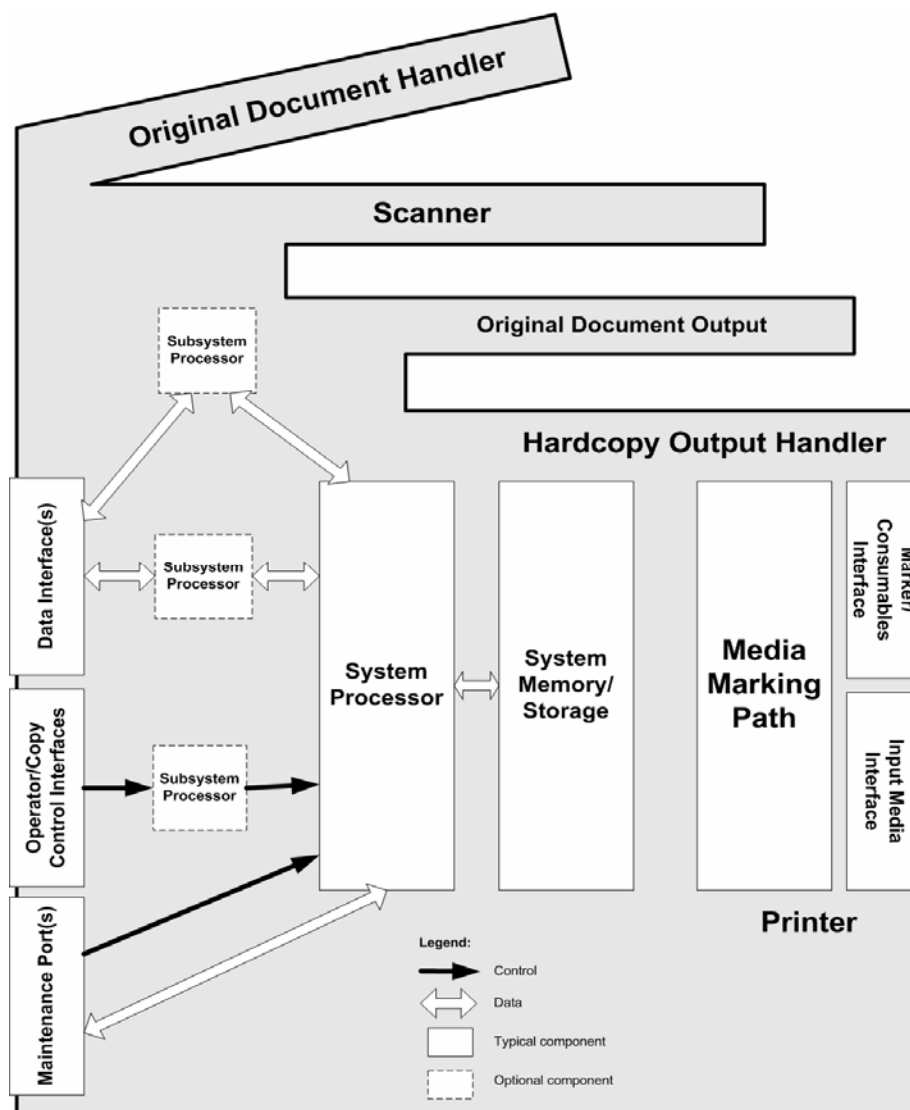


Figure 1—Generic architecture

3.2.1 Scanning function

3.2.1.1 Original document handler

The *original document handler* is the part of the HCD's media handling function that manipulates the input document into the proper position for scanning. Examples of Original Document Handler components include: flatbed glass window, single sheet feeder, or a multiple sheet input with duplexer.

3.2.1.2 Scanner

The *scanner* is an optical input device that uses light-sensing equipment to capture an image of a hardcopy document and translate it into a digital form that can be transmitted, stored, or be subsequently used to recreate the document.

3.2.1.3 Original document output

The *original document output* is the part of the HCD's media handling function that accumulates input documents after scanning.

3.2.2 Printing function

3.2.2.1 Input media interface

The *input media interface* includes any method for human access to the mechanisms that store and feed media (typically paper) to be marked on by an HCD. Examples of this interface would be the sliding drawers that hold paper for an office copier or the roll paper mechanism for a point-of-sale terminal.

3.2.2.2 Marker/consumables interface

The *marker/consumables interface* includes any method for human access to the user replaceable supplies (i.e., ink/toner/dye containers, developer roll, waste toner bottle) in an HCD. An example of this interface would be the doors and latches that are opened to replace a toner cartridge in a general-purpose laser printer.

3.2.2.3 Media marking path

The *media marking path* includes all paths in the printing function that the input media takes between the input media interface and the hardcopy output handler. This path may include certain intermediate media handling devices (e.g., duplexer) as well as the path through the marking mechanism.

3.2.2.4 Printer

The *printer* is the mechanism that applies ink, toner, or dye to create an image on the output medium. There are many different kinds of printers such as laser, LED, ink-jet, dot matrix, and dye sublimation. Depending on the kind of printer, they can create color output as well as black and white.

3.2.2.5 Hardcopy output handler

The *hardcopy output handler* is the part of the HCD's media handling function that holds or manipulates the media after it has exited the media marking path (print engine). The hardcopy output handler may also include certain post-printing processes (finishing options) such as stapling, folding, or hole punching. Examples include the exit tray of a printer, mailbox attachments to a MFD, and a stapler or collator attachment for a copier.

3.2.2.6 System processor and memory/storage

The *system processor* includes any microprocessor, digital signal processor, or microcontroller that has modifiable microcode or processes any type of user data or management information for the HCD. The *system memory* or *storage* includes any volatile or nonvolatile storage in the HCD. Examples include EEPROM, DRAM, SRAM, flash memory, and hard disk drive (HDD).

NOTE—Figure 1 shows the system processor or memory system as a single entity. In a typical HCD, many of the interfaces or components within a specific HCD may have their own microprocessor or memory subsystems.⁷

3.2.3 External interfaces

3.2.3.1 Data interface

The *data interface* of an HCD includes any interface that transports print or scan data into or out of the HCD's system processor and memory. Some data interface designs may include independent processor and memory subsystems. Examples include USB, parallel port (IEEE Std 1284-2000 [B43]), IEEE Std 802.3-2005 [B39], IEEE Std 802.5-1998 [B40], IEEE Std 802.11-2007 [B41].

NOTE—Some modular HCD architectures may include dedicated interfaces between specific functions of the device (e.g., scanner to print engine interface in an HCD, or a printing system where the system processor and memory are an external computer). These interfaces are not considered data interfaces in this standard.

3.2.3.2 Operator interface

The *operator interface* of the HCD is any physical human interface (e.g., touch screen LCD control panel) that allows access to the display or the modification of the state of the HCD. This interface can be as simple as a few lights and buttons on an inkjet printer to a full screen display with keyboard. This interface does not include remote or reflected user interfaces that may be implemented as part of a management application that accesses the device via one of the data interfaces. The remote management application and its host system are not within the scope of this standard.

3.2.3.3 Copy control interface

HCDs may include an electrical interface for external devices that are used for accounting, identification, or payment.

NOTE—This interface may also contain a software component as well.

3.2.3.4 Maintenance ports

Maintenance ports are interfaces used for machine maintenance, troubleshooting, and firmware updates.

3.3 Similarities and differences between HCDs and other IT devices

3.3.1 Basic security objectives for HCDs

Fundamentally, the security objectives for HCDs are the same as those for any kind of IT equipment that creates, stores, or processes information: protect the confidentiality, integrity, and availability of the defined assets.

HCD assets generally include but are not limited to the following:

⁷ Notes in text, tables, and figures of a standard are given for information only and do not contain requirements needed to implement the standard.

- a) The information being processed by the HCD
- b) Data that is associated with processing that information
- c) Data that is associated with configuring and securing the HCD
- d) Use of the HCD itself
- e) Physical assets associated with the HCD

See Clause 5 for complete definitions.

Security objectives also consider the confidentiality, integrity, or availability of the HCD's operating software and the data associated with authorizing HCD use and configuration, because their disclosure, alteration, or destruction can pose a threat to the HCD's assets. Additional security objectives consider the HCD's network services, because a misappropriated HCD could be employed to harm other IT devices on the same network.

See Clause 6 for more details.

3.3.2 Distinguishing characteristics

Many of the same administrative, physical, and logical security measures that are used to provide security for a general purpose computer can be applied to an HCD as well. However, HCDs are different from general purpose computers in the following ways:

- a) HCDs not only process and store a user's data in electronic form, they also process or generate a user's data in physical form when the documents are scanned or printed.
- b) HCDs have additional physical assets, such as toner or ink cartridges and blank media, intentionally designed for easy removal and replacement, which are required for the device to perform its intended function.
- c) By virtue of their intended function, HCDs may be more physically accessible than either a desktop computer or a server computer in a given environment, and they are often available for use by a larger number of users.
- d) HCDs are typically unattended, ownerless devices. Typically, desktop computers are placed in individual work areas and servers are placed in a controlled server room, but HCDs are often placed in common areas where they can be conveniently accessed by their users. In order to keep from disturbing people, HCDs are often placed out of sight from individual work areas and hence may be unmonitored for large periods of time.
- e) HCDs are a temporary receptacle for their users' current documents of interest, and even if those documents are encrypted in transit and storage, they are not necessarily encrypted during scanning, printing, copying, and PSTN faxing.

Each of these distinguishing characteristics has security implications that further distinguish HCDs from general purpose computers, as follows:

- 1) Physical hardcopy documents are physically submitted to or retrieved from the HCD. There are a number of ways that the physical document can be misappropriated, ranging from social engineering to compromising the HCDs security functions. Physical controls to mitigate these threats can be inconvenient and costly.

- 2) Physical assets such as toners or media can be stolen for their monetary value, compromised to degrade or deny use of the HCD, or altered to compromise the integrity of physical document output. However, since these assets are consumable, they are accessible to make it easy to replenish them.
- 3) Widespread physical access to HCDs implies a variety of threats and makes it more difficult to determine responsibility for security-related events, but limiting physical access to an HCD reduces its utility and its economy.
- 4) Unattended, out-of-the-way operation means that physical presence at an HCD can go unnoticed, and the expectation that HCD users need to be present to submit and retrieve jobs means that such presence is unlikely to arouse suspicion. The lack of an owner who might watch over an HCD compounds the situation, because people may not feel the authority to question another's presence.
- 5) Users are most likely to print, scan, copy, or fax their most important and most current documents, making the HCD an ideal target for espionage. Since documents cannot be encrypted when printed, scanned, or PSTN faxed, an HCD can also be a target for accessing documents that would otherwise be encrypted in storage and in transit.

3.4 Determining the appropriate security strategy for an HCD

3.4.1 Environmental factors

As with any IT system, the appropriate security measures for protecting an HCD largely depend upon the value of and risk to the assets being protected. This is commonly expressed in terms of the business impact if the asset is lost or compromised as well as the likelihood of an attack against that asset. For example, it may not be necessary to implement any particular security measures to protect the printing of a recipe for fried chicken in a typical home office, but an enterprise might implement extensive organizational, physical and technical measures to secure the printing of a recipe for fried chicken if that enterprise is a fast food chain and that recipe is a core asset. Similarly, an HCD in the heart of a military installation may require no security measures to protect user documents if it is used only to print the daily cafeteria menu. Clause 4 describes several generalized operational environments on which the guidance, recommendations, and requirements of this standard are based.

3.4.2 Regulatory factors

Many parts of the world have adopted blanket legislation that requires the protection of personal information. The European Union has adopted EU 95/46/EC [B21] that requires that parties “must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network and against all other unlawful forms of processing.” An almost exact directive has been adopted in Japan as well via the METI Policy on the Protection of Personal Information [B79].

Other countries have passed directives dealing with specific types of personal or personally identifiable information as well as some types of non-personal information. Among these specific directives are, in the U.S., the Gramm-Leach-Bliley Act [B27], which deals with the protection of personal financial information, and the Sarbanes-Oxley Act of 2002 [B141], which deals with the control and protection of corporate financial and accounting records. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) [B30] in the U.S., and the Personal Health Information Protection Act of 2004 (PHIPA) [B107] in Canada deal with the privacy and security of any type of personal “health related” information and details specific technical security measures, such as encryption, for protecting personal information in electronic form when transmitted or stored.

3.4.3 Typical approaches

3.4.3.1 General

For most operational environments, there is no global rule that defines which security measures are required or even warranted for an HCD. To help identify the appropriate security measures in a particular situation, the reader is directed to consult the following approach, which is most appropriate to their role.

3.4.3.2 For IT professionals

Each organization should perform a risk assessment that identifies assets, the threats to those assets, the probability of attack, and the business impact of a successful attack. Subsequently, the organization should compare the cost of mitigating each threat to the business impact of not mitigating the threat, and decide whether to mitigate, transfer, accept, or avoid that risk.

In some operational environments, specific procurement criteria, checklists, standards, or recommendations for securing IT equipment have been developed to aid in deciding what security measures to implement, thus reducing the need for a detailed risk assessment. Examples of some of these are provided in Clause 7, which may apply to HCDs if the assets of the HCD are sufficiently similar to the assets of the IT equipment.

3.4.3.3 For end users

If supported by an IT staff, end users should determine which of the operational environments in Clause 4 has been adopted by the IT staff, and then follow the appropriate guidance in Clause 7 and Annex A, regarding the use of their HCD. If unsupported, then end users should choose an appropriate security environment and follow its guidance.

3.4.3.4 For HCD manufacturers

The operational environments defined in Clause 4 are intended to be applicable to a variety of possible target markets. For a given target market, a manufacturer should choose the most applicable environment from the descriptions and examples given in Clause 4, and then should follow the guidance, recommendations, and requirements for that environment in Clause 7 and Clause 8, and in Annex A.

3.4.4 Use of this standard

3.4.4.1 Use by IT professionals

This standard is intended to help IT personnel determine an appropriate security strategy, but not to prescribe such a strategy. By identifying the operational environment in Clause 4 that most closely represents their particular HCD's environment, users of this standard will be guided to identify the appropriate assets described in Clause 5 and assess the relevant threats described in Clause 6, to perform their own risk analysis, and then consider the mitigation techniques described in Clause 7 and Annex A, to help decide how to handle their particular HCD security risks.

3.4.4.2 Use by end users

This standard is intended to help end users use HCDs in a secure manner through a combination of properly using the security features of their HCD and adopting secure behavioral practices, as described in Clause 7 and Annex A.

3.4.4.3 Use by HCD manufacturers

This standard is intended to help manufacturers design appropriately secure HCDs for a variety of operational environments. This standard will also help manufacturers provide default configuration settings and guidance to their customers to ensure that their HCDs are deployed and used in an appropriately secure fashion. By identifying the operational environments in Clause 4 that are most suitable to their customers, manufacturers will be guided to identify the appropriate assets in Clause 5, and design their products to protect those assets against relevant threats that are described in Clause 6.

4. Operational environments

4.1 Background

An organization's IT security needs depend on many factors, such as the value of its assets, the organizational impact of compromising those assets, the likelihood of a threat being carried out, various assumptions about the IT environment and about individuals in the organization, and externally mandated security requirements. The customary approach to evaluating a particular organization's IT security needs is to perform a risk analysis using those factors, and then a cost-benefit analysis to determine how (or whether) to mitigate each risk. There are many documented approaches to this process, including NIST Special Publication 800-30 [B82], ASIS International [B5], and ISO/IEC 27001:2005 [B71].

However, this standard is intended to apply to many different kinds of organizations, and so a conventional risk and cost-benefit analysis cannot be performed. Instead, four generalized classes of operational environments are defined. These environments are adapted from NIST Special Publication 800-70 [B102]. By choosing a generalized environment that most closely matches a particular organization's specific environment, the organization can identify the guidance and recommendations that are most applicable to its specific needs. Similarly, by choosing the generalized environment that most closely matches the requirements of a particular manufacturer's target customers, that manufacturer can identify the recommendations and requirements that are most applicable to that target market. Four operational environments (A, B, C, and D) are considered in this standard.

4.2 Operational Environment A

4.2.1 Description

Operational Environment A is generally characterized as a restrictive information processing environment in which enhanced document security, operational accountability, and information assurance are required. Typically, such systems process confidential information (e.g., personnel records, medical records, and financial information) or perform mission-critical and vital organizational functions (e.g., accounting, payroll processing, and insurance claims), and process supervisory control and data acquisition (SCADA) related documents or documents with high intellectual property value. HCDs in this environment might be targeted by third parties for exploitation, and they may be targeted by trusted parties inside the organization. This environment is not intended to support life-critical or national security applications, which are out of scope for this standard.

Operational Environment A may be appropriate for medium to large businesses, some governmental agencies, and organizations requiring tightly managed telecommuting systems and remote offices. These organizations typically have a group of IT professionals dedicated to supporting users and providing security. The combination of structure and skilled staff allows better security practices to be implemented during initial system deployment and in ongoing support and maintenance. The managed nature of typical enterprise environments gives administrators centralized control over various settings on workstations, servers, hardcopy and other types of devices, as well as the sharing of resources (e.g., file servers, printers). Environments like Operational Environment A enable only the services needed for normal business operations, with other possible avenues of exploit removed or disabled. Authentication, account, and policy management are administered centrally to maintain a consistent security posture across an organization.

This environment may include telecommuters who connect to an enterprise network from home or other remote locations and whose connection and equipment are tightly managed by the enterprise's IT department.

See Figure 2 for an infrastructure architecture typical of Operational Environment A. As an example, it would include networked printers and MFDs, managed workstations, and internal servers.

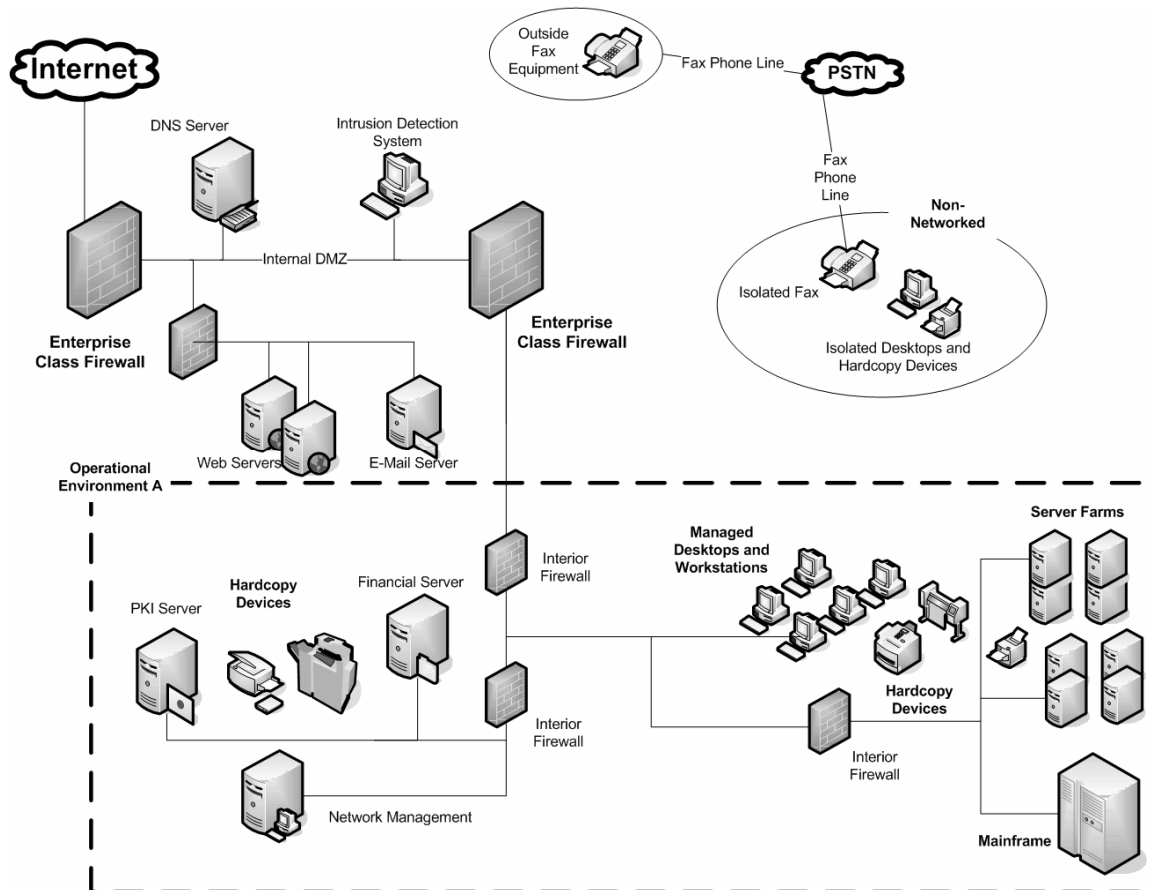


Figure 2—Operational Environment A example

Operational Environment A could also describe a subset of equipment located within another environment. For example, three desktops in a corporate enterprise that hold confidential employee data could be thought of as an Operational Environment A island within a typical enterprise (Operational Environment B) environment. Another example might include a laptop used by a mobile worker that is an Operational Environment A island within a typical small office/home office (SOHO) (Operational Environment D) environment. This environment might also be a self-contained environment outside any other environment, such as a credit card processing operation.

4.2.2 Typical security environment

Threats from insider attacks are equal to and often of greater concern than external attacks. Systems may have permanent, well-known IP addresses and name spaces with high visibility to attackers. Systems may be subject to automated intrusions and denial of service (DoS) attacks, as well as manual intrusions. Penetrations of firewalls and servers could lead to local attacks and intrusions. Local threats may be elevated if the systems are connected to large networks with many users or may be less if connected to

smaller networks. Because of the risks and possible consequences of a compromise, this environment usually has the most functionally restrictive and secure configuration described in this standard. The suggested configuration provides the greatest protection with considerable tradeoffs to ease of use, functionality, and remote system management.

The following general practices and controls are likely to be found in Operational Environment A:

- a) Systems generally process as few types of data as possible (i.e., do not combine multiple server applications on the same system)
- b) Systems are stripped of all unnecessary services and applications
- c) If possible, host-based firewall applications are used
- d) Systems have as few users as possible
- e) Strong authentication is used (e.g., authentication token, biometrics, smart cards)
- f) Remote administration or access is restricted; if used, connections are encrypted
- g) Security-related OS and application patches and updates are tested and applied as soon as possible
- h) Systems are placed behind firewalls and other network security devices to restrict access and filter unnecessary protocols
- i) Intrusion detection and other logs are monitored on a frequent basis
- j) Vulnerability assessment tools are run against the systems on a frequent basis
- k) System administrators are highly skilled in the appropriate technologies
- l) Physical security is regularly assessed and updated

4.2.3 Examples

The examples that follow describe typical HCD environments that might be considered Operational Environment A.

Pharmaceutical research lab—Internet access is provided in these facilities with tightly controlled firewalls or proxies. E-mail may be provided. The research data produced, stored, and used is of high value. Internal networks may potentially be segregated from other internal networks and some of these segregated networks may not be connected to the Internet. Enhanced physical security is present. Employees may have been cleared through some screening process before given access to the high value information. Visitors are tightly controlled. There is a high potential for industrial espionage.

Bank/financial/stock broker—In this environment there is often moderate physical security and escorts are required when in the facility. There is often no Internet connection or the electronic assets may be segregated onto a private network. E-mail is provided although generally through a secure server that prevents the outflow of certain types of information and attachments. Foreign devices [personal computers (PCs), personal digital assistants (PDAs), etc.] are often not allowed on the network and a private wide area network (WAN) connection is used for electronic communication among remote offices. The assets, many individuals' private financial information, are subject to legislative privacy requirements.

Health insurance claims processing—This environment can include moderate physical security as there is little need for non-employees to be present. Outsiders can be controlled and escorted to prevent malicious acts. The IT environment may include multiple ports of electronic entry to support claim submissions from health care providers, e.g., fax, Internet, point-to-point. Funds transfer and other sensitive information will flow out of this office back to doctors, hospitals, pharmacies, and other health care providers. Additionally, the production printing systems will generate substantial sensitive information in the form of claim acknowledgements and claim reports that will be mailed to the provider and the patient but is required to be reasonably protected before being given to the postal service. IT services are typically provided in-house or by an outsourced provider. These technicians are reasonably skilled and the network can be protected by appropriate firewalls and segmentation.

Doctor's office—The office of a one or two doctor practice is typically located in a highly accessible, small or medium office building. With the exception of certain medicines and drugs, physical security is often minimal. A third party not located in the practice often provides support for the IT equipment. The skill level of these third-party providers can vary drastically. Connectivity to the Internet for e-mail, research, and insurance claim submission may be present. In some countries, all health providers are required to safeguard patient records (HIPAA in the U.S., PHIPA in Canada, and similar legislation in other countries). Improved guidance regarding HCD threats and risks may be required for small businesses processing valuable assets in environments with minimal physical security. Products with appropriately aggressive security features should be considered despite the scale of the business.

Hospital—The facility is typically a relatively large building or campus with a large population of networked HCDs. While there is some security, visitors are everywhere and there is constant outsider interaction with administrative and medical personnel. Nursing stations may have small exposed HCDs and temporary help in the form of volunteers with access to most areas is common. IT equipment may be provided and supported by a third party but large facilities typically have their own IT staff. The security savvy of the third-party providers can vary drastically, and IT staff awareness of HCD vulnerabilities is often low. Connectivity to the Internet for e-mail, research, diagnostic test results, and insurance claim submission may be present. In most countries, all health providers are required to safeguard patient records (HIPAA in the U.S., PHIPA in Canada and similar legislation in other countries) as well as confidential patient financial information, and ID information. Also at risk is audit and record information that frequently plays a role in court cases.

Local district attorney's office—As a government office, unescorted access to public areas within these offices is required. Therefore only a moderate level of physical security can be implemented. The assets contained in this office are printed material (or electronic versions of the same) related to criminal and civil legal proceedings, which may not be public and are generally highly confidential. Public access to public records of this office via the Internet is required so Internet connections are present. Non-public document processing resources are isolated since they meet the definition of assets in need of strong protection. Firewalls and proxies are generally used. E-mail is broadly available.

Social Security office—Similar to the preceding district attorney's office, many Federal government offices and agencies like the Social Security Office are open with easy access for all people. Additionally, to communicate with their clients, employees of the office have Internet e-mail capability. Information available on the Social Security office network is highly sensitive. This information includes personal information such as the salary history used to calculate benefits. It may also include medical information such as documentation necessary to support disability claims and other similar information.

Power and light company facilities—Recent U.S. Dept. of Homeland Security (DHS) initiatives counsel commercial enterprises that manage critical infrastructure to address weak links in their networks that might enable DoS attacks and impair the network's ability to respond in a timely fashion in emergency situations. Administrative areas supporting maintenance and operation of critical power and communication systems and controlling access and personnel availability and records pertaining to support systems are all processed by HCDs. Access to outside communication networks is often controlled and network vulnerabilities that might impact availability and response times are typical concerns. Additionally, those who manage nuclear power plants have areas that are required to follow Nuclear

Regulatory Commission (NRC)/U.S. Dept. of Energy (DOE) regulations and place their HCDs in the more secure, high asset value category described by Operational Environment A. IT staff typically seeks a uniform solution for the network; however, some policies and practices throughout the network require that all assets at risk be assigned a high value given their potential public impact.

Telephone network and switch company facilities—Similarly to the power and light company facility example, commercial organizations that may not be governed by current legislation from a security perspective may place their customer base at risk through the disclosure of personal communications records documents and by not taking adequate measures to assure that their administrative systems do not pose a threat to their ability to deliver critical public communication services at all times. Network DoS attacks and unauthorized access to configuration, management, support, and service documents processed by HCDs are issues of increasing concern. HCDs used in the communications support facilities that blanket the country face threats and deal with assets typical of Operational Environment A.

SCADA systems—The preceding power and communications user examples address high profile SCADA system threats. Commercial organizations involved in major public transportation systems, delivery and transport of critical fuels, and those who manage similar networks that might have widespread public impact if directed should consider deploying hardcopy document resources that meet the Operational Environment A requirements in areas where critical control and support systems might be jeopardized.

4.2.4 General security expectations for Operational Environment A

The security related expectations of an HCD that is used in Operational Environment A are necessarily high due to the expectation that the type of information that might be processed by the HCD is of significant value to the *user* or the *user's operational environment*. Even though the physical security expectations for this environment are also high, HCDs also are expected to provide robust security functions in this environment. These expectations include the following:

- All *users* and *administrators* of the HCD are identified and authorized before being able to use or access the capabilities of the HCD. This includes accessing via any type of network or local data connections, as well as any type of user interface. Note that inbound fax connections to an HCD may not be able to completely meet this expectation due to the fact that it is, by design, an unauthenticated, anonymous data connection.
- HCDs are expected to provide protection for user's documents from unauthorized disclosure, modification, or access. This expectation extends not only to the user's document while it is being processed or stored within the HCD, but also any electronic transmission of an authorized user's document to or from the HCD. Additionally, certain information about the user's document or the processing of that document, e.g., number of copies, duplex, color settings, is expected to be protected from unauthorized modification while both stored and in transit.
- HCDs are expected to provide protections against the disclosure of residual user document information that may reside in the HCD after the processing of that user document is completed.
- HCDs are expected to provide protection for any internal HCD configuration parameters, settings, logs, or other HCD specific security related information from unauthorized modification (and unauthorized access for certain types of security related information and logs). This expectation extends to any transmission of this information to or from the HCD as well as while it is resident in the HCD.
- HCDs are expected to provide protection for any internal HCD software, firmware, or other digital resources (e.g., downloadable fonts, images, forms) from unauthorized alteration (including deletion), while resident in the HCD.
- HCDs are expected to monitor and record, via protected logs, any security relevant events that occur within the HCD. Examples of these types of events might include: successful and

unsuccessful authentication attempts, changes in security relevant settings on the HCD, or changes in the content or state of the HCD's internal security or accounting logs.

- HCDs are expected to monitor and record, via protected logs, any use of HCD functions. Examples of these types of events might include: printing a document, scanning a document, receipt of a fax, etc.
- HCDs are expected to participate in networked and other shared-medium environments in a robust and orderly manner. This expectation includes resilience in the face of network-based DoS attacks as well providing mechanisms that reduce the likelihood that the HCD will interfere or obstruct the function of the network or other networked devices.

4.3 Operational Environment B

4.3.1 Description

Operational Environment B is generally characterized as an information processing environment in which a moderate level of document security, network security, and security assurance are required. Typically, this environment will handle the day-to-day proprietary and non-proprietary information needed to operate an enterprise. Figure 3 shows an example network architecture typical of Operational Environment B, which includes networked printers and MFDs, managed workstations, and internal servers.

Operational Environment B may be appropriate for medium to large businesses, some governmental agencies, and organizations requiring managed telecommuting systems and remote offices. These organizations typically have a group of IT professionals dedicated to supporting users and providing security. The combination of structure and skilled staff allows better security practices to be implemented during initial system deployment and in ongoing support and maintenance. The managed nature of typical enterprise environments gives administrators centralized control over various settings on workstations, servers, hardcopy and other types of devices, as well as the sharing of resources (e.g., file servers, printers). Environments like Operational Environment B enable only the services needed for normal business operations, with other possible avenues of exploit removed or disabled. Authentication, account, and policy management can also be administered centrally to maintain a consistent security posture across an organization. This environment includes telecommuters who connect to an enterprise network from home or other remote locations and whose connection and equipment are managed by the enterprise's IT department.

Environments described in this subclause may have a mixture of operational environments. It is common to have *islands* within all of the environments described that contain assets of high value and HCDs that process critical information requiring Operational Environment A precautions. The example in Figure 4 suggests an office such as a personnel department, a legal department, a research and development office, or a corporate executive office that require a higher degree of isolation and access control within a corporate enterprise typical of Operational Environment B. Islands of this type frequently have increased physical security restricting office access or building access. Also shown is a secured home office; this is an example of an Operational Environment A installation in a location that might usually be Operational Environment D.

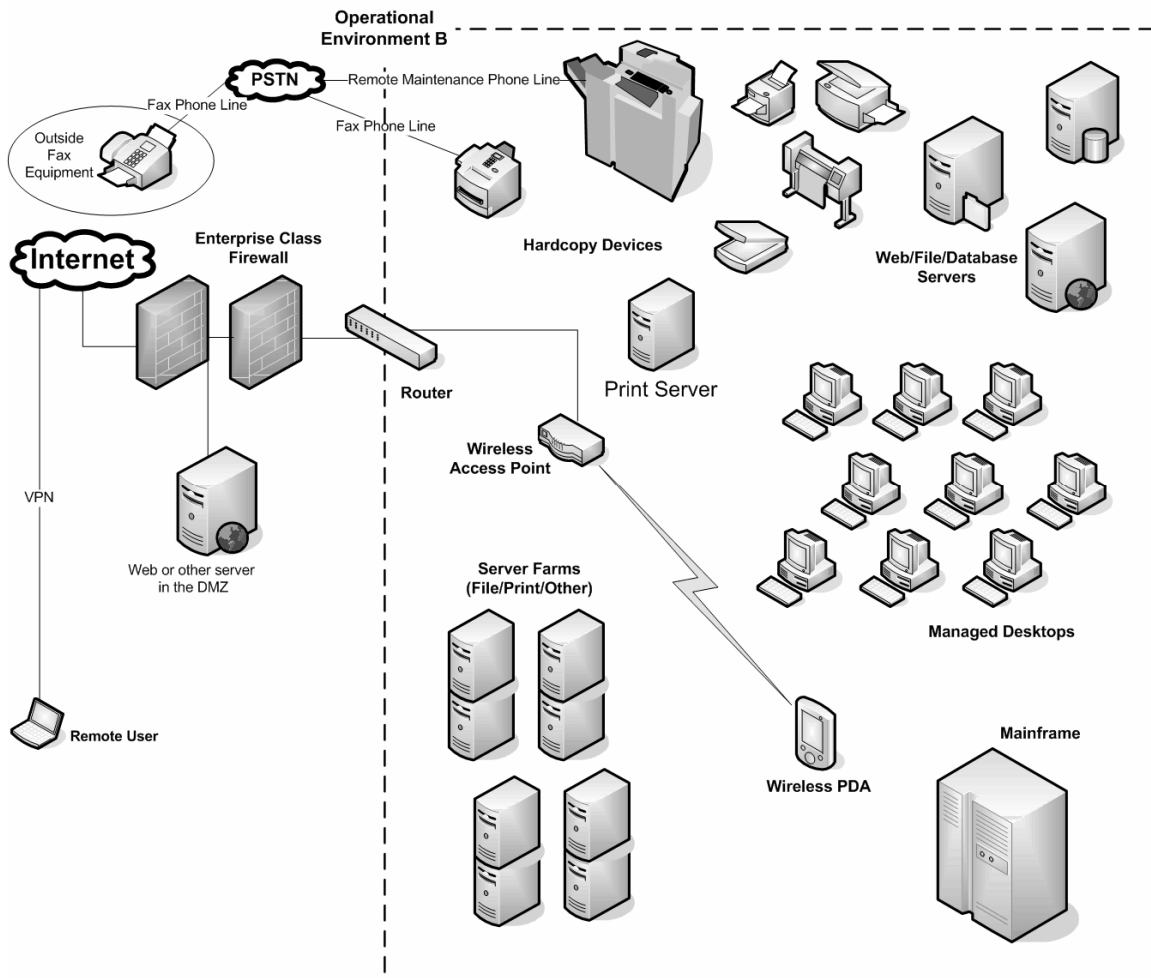


Figure 3—Operational Environment B example

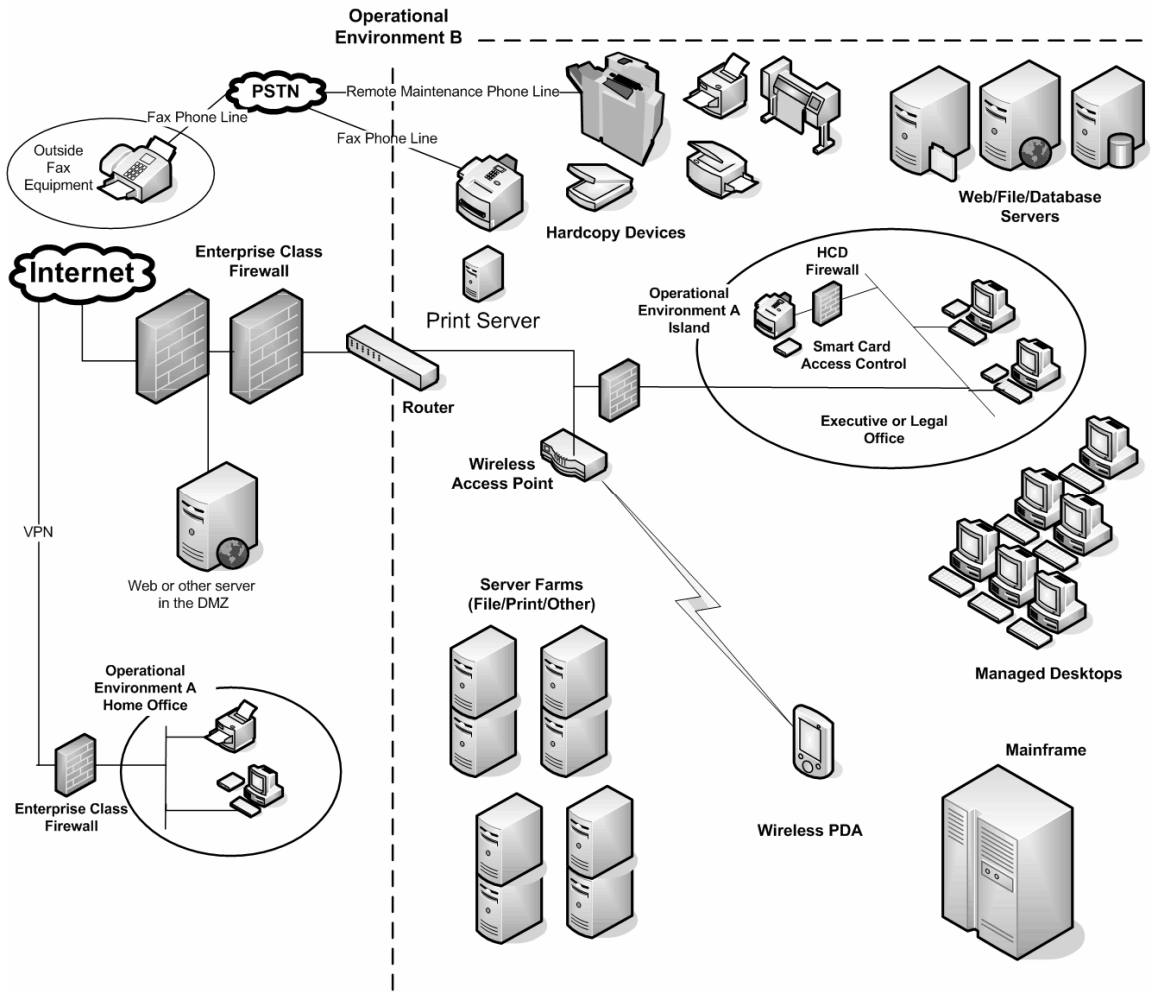


Figure 4—Centrally managed Operational Environment B with Environment A islands

4.3.2 Typical security environment

Systems in this environment face many of the same threats as systems in Operational Environment A. Remote and local threats to Operational Environment B networks could have significant impacts to systems and applications. Enterprise organizations often have systems and devices with permanent, well-known IP addresses and name spaces with high visibility on the Internet to attackers. Most systems on enterprise networks are usually inward-facing—protected from direct exposure to the Internet by firewalls—but penetrations of those systems through other means could permit intruder access to internal networks. For example, viruses and worms could spread across homogenous networks in a short amount of time. Also, in these environments, the insider threat is generally greater due to the larger number of users and lower strength of authentication than one finds in Operational Environment A.

In environments like Operational Environment B, systems are typically susceptible to both local and remote threats. Local attacks, such as unauthorized usage of another department's workstations or HCDs, can often lead to unauthorized access to data, but may also lead to unauthorized data modification or consumption of resources. Remote threats may be posed not only by attackers outside the organization, but also by local users who are attacking other local systems from within the organization's network. Most security breaches caused by remote threats involve malicious payloads sent by external parties, such as viruses and worms acquired via e-mail or infected Web sites. Threats against network-based applications tend to affect a

smaller number of systems and may be caused by internal or external parties. Both malicious payloads and network application attacks are most likely to affect availability (e.g., crashing the system or device, consuming all network bandwidth, breaking functionality) but may also affect integrity (e.g., infecting data files) or confidentiality (e.g., providing remote access to sensitive data). Data disclosure threats tend to come from internal parties who are monitoring traffic on local networks, and they primarily affect confidentiality.

Some commonly accepted security practices found in Operational Environment B are as follows:

- a) Internal networks are segmented with internal firewalls and other defense-in-depth techniques
- b) System management is centralized with restricted access to management functions
- c) Security-related applications (e.g., antivirus) are centrally managed
- d) Installation of system and application patches and updates is automated
- e) Access to printer and MFDs and their features is restricted, and accounting features are enabled
- f) Unnecessary ports and protocols are disabled
- g) Backup and recovery facilities are centralized

4.3.3 Examples

The examples that follow describe typical HCD environments that might be considered Operational Environment B.

High-tech international company—Product plans, company intellectual property, printing, and scanning of documents to and from overseas manufacturing and support groups requires an increased focus on the security of document handling resources. Enterprise networks today link global sites and create new opportunities for attacks. Increased use of outsourced personnel with limited background data also raises the threat of internal attacks. While islands in large enterprises justify the use of Operational Environment A, the baseline for every large corporation with considerable assets at risk is Operational Environment B, which is intended to provide security recommendations applicable to all corporate enterprises with tangible assets.

Advertising agency/PR agency/photographic studios—Promotional and advertising companies today can be large global operations with numerous high profile clients. Typically, confidential information associated with product and events not yet disclosed to the public that might have significant financial repercussions are disclosed in detail to these organizations. Specifications are copied and product information printed, scanned, and exchanged with project teams. Corporate project teams in foreign locations review and exchange hardcopy materials associated with the products and projects. Industrial, corporate, and international espionage threats can be mitigated by prudent and more secure use of office resources such as the HCDs that process all the documents at risk.

Cable television company—Broadcast media companies have also become communication companies providing two-way data services and even audio-video services over their networks. Client financial information and access information for thousands of subscribers may be processed by office HCDs. Care should be taken to eliminate the possibility of remote access to the office document handling systems since the cable network itself will likely have a large number of sophisticated potential attackers linked to the servers providing public access. Personally identifiable information providing access to Internet-based services may be at risk.

Large retail firm—Retail operations today frequently provide their own credit services and manage a large database of customer personal and financial information. This is especially true of companies dealing with larger, frequently financed items such as furniture outlets and large electronics retailers. Customer financial information is frequently processed by the company hardcopy resources that have the potential to put client information at risk.

College campus—The college campus environment is a special case of Operational Environment B and includes broad access to and from the Internet; however, there are several unique differences. First, because of academic freedom issues, there tends to be less content filtering and other protections in use. Students and staff need to be able to accomplish a wide range of tasks that are difficult to characterize and therefore configuration of protection devices and systems have to allow for a broad range of usage. Second, due to the age and maturity levels of some college students, the campus IT environment is often viewed as a challenge. These students are often very motivated insider attackers who constantly search for systems to compromise. A college's HCDs may be accessible to a large number of unscreened individuals in work-study programs and other volunteer work.

4.3.4 General security expectations for Operational Environment B

Although not as high as the expectations for Operational Environment A, the security related expectations of an HCD in Operational Environment B still require the HCD to provide a robust level of security for the types of information being processed. These expectations include the following:

- All users and administrators of the HCD are identified and authorized before being able to use or access the capabilities of the HCD. This includes accessing via any type of network or local data connections, as well as any type of user interface. Note that inbound fax connections to an HCD may not be able to completely meet this expectation due to the fact that it is, by design, an unauthenticated, anonymous data connection.
- HCDs are expected to provide protection for user's documents from unauthorized disclosure, modification, or access while it is being processed or stored within the HCD. Additionally, certain information about the user's document or the processing of that document, e.g., number of copies, duplex, color settings, is expected to be protected from unauthorized modification while stored in the HCD.
- HCDs are expected to provide protections against the disclosure of residual user document information that may reside in the HCD after the processing of that user document is completed.
- HCDs are expected to provide protection for any internal HCD configuration parameters, settings, logs, or other HCD specific security related information from unauthorized modification (and unauthorized access for certain types of security related information and logs). This expectation extends to any transmission of this information to or from the HCD as well as while it is resident in the HCD.
- HCDs are expected to provide protection for any internal HCD software, firmware, or other digital resources (e.g., downloadable fonts, images, forms) from unauthorized alteration (including deletion), while resident in the HCD.
- HCDs are expected to monitor and record, via protected logs, any security relevant events that occur within the HCD. Examples of these types of events might include: successful and unsuccessful authentication attempts, changes in security relevant settings on the HCD, or changes in the content or state of the HCD's internal security or accounting logs.
- HCDs are expected to monitor and record, via protected logs, any use of HCD functions. Examples of these types of events might include: printing a document, scanning a document, receipt of a fax, etc.

- HCDs are expected to participate in networked and other shared-medium environments in a robust and orderly manner. This expectation includes resilience in the face of network-based DoS attacks as well providing mechanisms that reduce the likelihood that the HCD will interfere or obstruct the function of the network or other networked devices.

4.4 Operational Environment C

Operational Environment C is generally characterized as a public-facing environment in which document security is not guaranteed, but access control and usage accounting are important to the operator of the environment. A retail copy center, public library, Internet café, and hotel business center are typical examples of this environment.

4.4.1 Typical environment

These organizations typically have a group of IT professionals dedicated to supporting users and providing security. The combination of structure and skilled staff allows better security practices to be implemented during initial system deployment and in ongoing support and maintenance. The managed nature of these environments gives administrators centralized control over various settings on workstations, servers, hardcopy and other types of devices, as well as the sharing of resources (e.g., file servers, printers). Environments like Operational Environment C should enable only the services needed for normal business operations, with other possible avenues of exploit removed or disabled. Authentication, account, and policy management can also be administered centrally to maintain a consistent security posture across an organization. This environment does not typically include telecommuters who connect to an enterprise network from home or other non-business remote locations.

The typical Operational Environment C environment is a business or public sector operation that provides some combination of wired and wireless Internet connectivity, desktop computers, and HCDs, for general use by transient patrons, members, customers who pay a service rental fee, or the general public. This environment is likely to have some or all of the following characteristics:

- a) Due to its public nature, it is difficult to provide physical security.
- b) Since the users of these services are transient, it is impractical to manage user identities and accountability in the way one would in Operational Environment A or B.
- c) There may be requirements that usage is granted to those who have some kind of permission, that device and security settings are controlled, and for which resource usage is accounted.
- d) This environment may also have some connection to a more controlled environment that manages access control, performs billing functions, supplies read-only access to databases, or performs other functions.
- e) There may be a high risk of, and associated controls for, local injection of viruses or worms and other uses that violate terms of service.
- f) Because of its public nature, the typical instance of Operational Environment C may not assure any kind of document security. However, its operator may wish to add value by providing some level of document security and should therefore consider adopting some of the security objectives of Operational Environment B.

4.4.2 Examples

The examples that follow describe typical HCD environments that might be considered Operational Environment C.

Public library—One example of Operational Environment C is a public library, as shown in Figure 5. Patrons in the public library are able to use the public computers as well as the public copiers, printers, and scanners. This is public space with no physical security during business hours. Internet access and e-mail are often available both to the public and to the employees. Libraries are not liable for disclosure of copied, scanned, or printed content. Accurate charge-back and payment information is required to recover the costs of fair use duplication of material. No credit card information is retained by the HCD after a transaction.

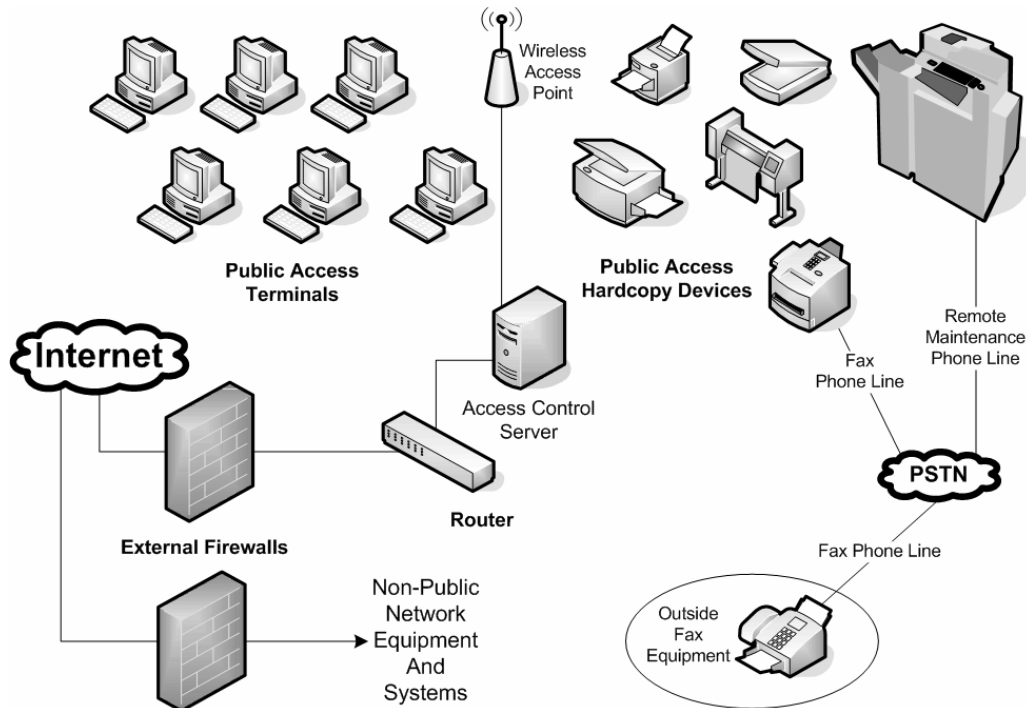


Figure 5—Operational Environment C example—public library

Hotel business center—Many large hotel chains provide visitor access to HCDs with print, copy, fax, and scan capabilities. Some provide remote access from hotel rooms to these resources. Typical users are business travelers with the need to process hardcopy based information that might be confidential company information or personal information.

Retail copy shop or Internet café—This is intended to be used by the public; therefore no physical security is present during business hours. Wireless Internet access may be provided to patrons for a nominal fee or no fee. PCs and HCDs with wired access may also be provided. The business' operations network (non-public) will be segregated or firewalled from the public network. Credit card information is present on the operation's network but not generally through any HCD. The openness of these environments suggests that they are high risk with minimal security. Deployment of security tools typical of, for example, Operational Environment A would constrain user access and is generally not feasible: user caution is advised.

4.4.3 General security expectations for Operational Environment C

The security related expectations of an HCD in Operational Environment C focus on the integrity and security of the configuration and function of the machine and not necessarily the security of the information being processed by the HCD. This narrowing of expectations centers on the fact that this environment is focused on publicly accessible and publicly used HCDs where a user should not expect robust protection of the information being processed. These expectations include the following:

- All administrators of the HCD are identified and authorized before being able to access the administrator functions of the HCD. This includes accessing via any type of network or local data connections, as well as any type of user interface.
- HCDs are expected to provide protections against the disclosure of residual user document information that may reside in the HCD after the processing of that user document is completed.
- HCDs are expected to provide protection for any internal HCD configuration parameters, settings, logs, or other HCD specific security related information from unauthorized modification (and unauthorized access for certain types of security related information and logs). This expectation extends to any transmission of this information to or from the HCD as well as while it is resident in the HCD.
- HCDs are expected to provide protection for any internal HCD software, firmware, or other digital resources (e.g., downloadable fonts, images, forms) from unauthorized alteration (including deletion), while resident in the HCD.
- HCDs are expected to monitor and record, via protected logs, any security relevant events that occur within the HCD. Examples of these types of events might include: successful and unsuccessful authentication attempts, changes in security relevant settings on the HCD, or changes in the content or state of the HCD's internal security or accounting logs.
- HCDs are expected to participate in networked and other shared-medium environments in a robust and orderly manner. This expectation includes resilience in the face of network-based DoS attacks as well providing mechanisms that reduce the likelihood that the HCD will interfere or obstruct the function of the network or other networked devices.

4.5 Operational Environment D

4.5.1 Description

Operational Environment D is generally characterized by a small, private information processing environment in which many elements of security are provided by the physical environment. Some level of network security is needed to protect the device and its network from misuse originating outside of the environment. Small offices and home offices are typical examples of this environment. Figure 6 shows a typical Operational Environment D environment.

The following are typical characteristics of the target end-user audiences and configurations:

- a) Home users with stand-alone systems, generally with dial-up or high-speed access to the Internet, possibly using wired or wireless home networks, possibly sharing resources across the networks.
- b) Telecommuters using stand-alone systems who work from a home office but who are not operating under the control of an enterprise IT department, i.e., not Operational Environment A or B islands.

- c) Small businesses, typically with small networks of stand-alone desktop systems and small office servers, protected from direct Internet access by a firewall, but possibly including some small centrally managed networks of desktop systems and products, and typically not maintaining publicly accessible servers.
- d) HCDs may be directly connected using IEEE 1284, Universal Serial Bus (USB), or other local connectivity, to desktop computers, general purpose servers, or print servers. Devices connected to one system can be shared with other systems. In some environments, these HCDs are directly connected to the network using Ethernet, IEEE 802.11, HomePNA™,⁸ or similar networking technologies.

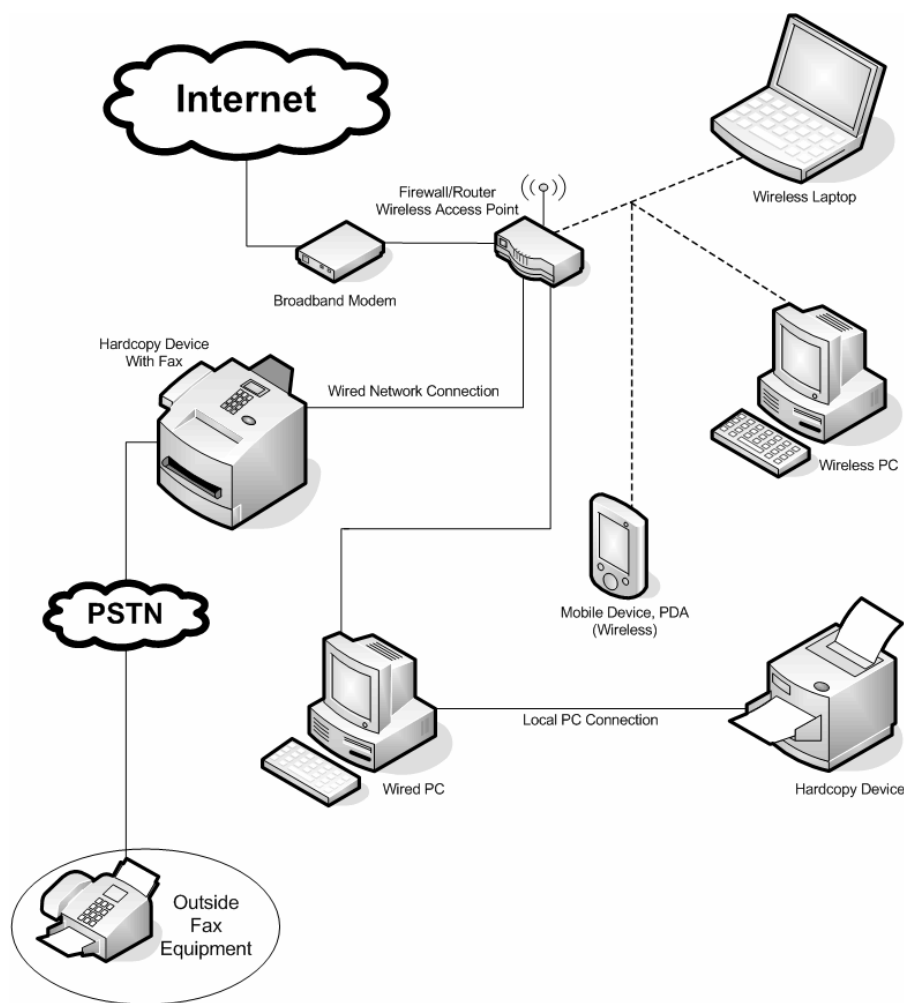


Figure 6—Operational Environment D example

4.5.2 Typical security environment

Operational Environment D is typically the least secured of the environments considered in this standard. The individuals performing small office or home office system administration are assumed to be less knowledgeable about security than enterprise system administrators. This often results in environments that

⁸ HomePNA is a trademark of the HomePNA Alliance [B32]. This information is given for the convenience of users of this standard and does not constitute an endorsement by the IEEE of these products. Equivalent products may be used if they can be shown to lead to the same results...

are less secure than they should be because the system administrator's focus is on functionality. There may be no network-based security controls such as firewalls, or those present may be out-of-date or ineffective, thereby directly exposing the network and devices to external attacks. These environments are frequently targeted for exploitation to acquire information through keystroke logging or other phishing methods, to perform distributed DoS attacks on other computers, to deliver spam e-mail messages, or to propagate viruses or worms. Systems in this environment may themselves be infected by viruses or worms, or suffer collateral damage resulting from malicious software installation and use.

Because the primary threats in this environment are external, and the HCD devices deployed generally have less restrictive security policies than those in Operational Environment A or B, they tend to be most vulnerable to attacks from remote threat categories. Local threats are often less significant because few people typically have local access to personal or small business systems; however, it is still important to protect against local and other threats. Systems for Operational Environment D are typically exposed to attacks against network services and by malicious payloads (e.g., viruses, worms). These attacks are most likely to affect availability (e.g., crashing the system, consuming all network bandwidth, breaking functionality) but may also affect integrity (e.g., infecting data files) and confidentiality (e.g., providing remote access to sensitive data, e-mailing data files to others).

Operational Environment D networks often have the following characteristics:

- a) Consumer-class hardware Internet firewall appliances are used to block inbound connections and possibly to also filter outbound traffic.
- b) Some systems may have host-based firewalls.
- c) Computers are likely to have antivirus software and possibly anti-spyware software. The engines and definition files associated with these programs may be out-of-date.
- d) There may be a mixture of OSs present; including some that may be no longer supported with security updates. OS updates or patches, if available, may not necessarily be applied in a timely fashion.
- e) Systems are likely to be left in their out-of-box configuration, which can mean that unnecessary applications, services, and protocols remain enabled and not configured beyond their original state.
- f) Network encryption is seldom used.
- g) Wireless LANs may be unsecured, may use older, less secure protocols, may use weak keys, or may use default configurations that can easily be compromised.
- h) User accounts, if used at all, may have weak or no password protection.
- i) Shared resources are likely to have few access controls.

4.5.3 Examples

The examples that follow describe typical HCD environments that might be considered Operational Environment D.

Real estate broker—These are generally in small-to-medium office buildings located in highly accessible locations. There is no substantial physical security. E-mail and Web access are required and often with only minimal firewalls on the Internet connection. The susceptible assets are generally land and building

contracts and other agreements. Some may have accounting considerations. Few, if any, legislative privacy or other controls are required or observed.

Architect's office—These offices are generally in small-to-medium office buildings with no substantial physical security. Internet access and e-mail are available often with only minimal firewalls on the Internet connection. The susceptible assets usually do not include private information but do include business information such as cost estimates, schedules, plans and drawings, supplier and contractor contact information, customer lists, and other confidential business information.

Home—Only trivial physical security, such as door locks, is present. The assets could be confidential and consist of personal and financial information. Internet access and e-mail are commonly present through dial-up or increasingly through always-on broadband connections. Wireless networks are increasingly common and often not protected with WEP, WPA, IEEE 802.11i™, or any other security techniques. Firewalls and proxies are often not present. There are no legislative mandates to protect one's own information from attack.

4.5.4 General security expectations for Operational Environment D

The security related expectations of an HCD in Operational Environment D focus on the integrity and security of the configuration and function of the machine and not the security of the information being processed by the HCD. These expectations include the following:

- All administrators of the HCD are identified and authorized before being able to access the administrator functions of the HCD. This includes accessing via any type of network or local data connections, as well as any type of user interface.
- HCDs are expected to provide protection for any internal HCD configuration parameters, settings, or other HCD specific security related information from unauthorized modification (and unauthorized access for certain types of security related information) while stored in the HCD or in transit.
- HCDs are expected to provide reasonable protection for any internal HCD software or firmware from unauthorized alteration while resident in the HCD. At a minimum, the HCD is expected to indicate to the administrator or user that change has occurred.
- HCDs are expected to participate in networked and other shared-medium environments in a reasonably robust and orderly manner. This expectation includes providing at least minimal protections that reduce the likelihood that the HCD will interfere or obstruct the function of the network or other networked devices.

4.6 Choosing the most applicable operational environment

When choosing the most applicable environment to use as a guide for particular security needs, the reader should look beyond the simple description of the environment and instead consider both the totality of the operational environment and the value of the most valuable assets to be protected. Table 1 summarizes those factors for each environment.

Table 1—Factors affecting security

Operational Environment	Effect on security requirements			
	A	B	C	D
Element of security				
Value of asset	High	Moderate	Moderate–Low	Low
Physical security	High	Moderate	Low	Low
Network protection	High	Moderate	Moderate	Low
Laws and regulations (see Note)	High	Moderate–Low	Low	Low
Personnel trust	High	Moderate	Low	Low
NOTE—Laws and regulations include privacy and governance laws, industry-specific standards, etc.				

Here are some examples of how an appropriate operational environment might be chosen:

Home appliance service company—This business typically has a network of computers to run their operation, which includes taking orders, dispatching trucks, general bookkeeping, and providing access to service documentation. Operational Environment B is the most applicable environment description. However, a few of the company's routine functions involve private information such as credit card processing for customers and payroll and health insurance records for its employees. Systems that perform those functions are likely to be regulated by laws and would therefore need to be considered as Operational Environment B with islands of Operational Environment A.

Publicly traded pharmaceutical manufacturer—This business performs many functions that are regulated or involve highly valuable competitive information. For example, their bookkeeping is regulated by governance laws, their clinical trial data is regulated by privacy laws, and their research and patent data is so valued that its disclosure could result in the loss of significant future revenue. All of these activities would clearly require the precautions typical of Operational Environment A. However, there are many other functions in the company that are not regulated nor involve trade secrets. For example, they have an in-house corporate travel service, cafeteria food service for employees, fleet management for company vehicles, and a worldwide distribution center.

Home user—A typical home network often consists of two desktop computers and an HCD, which is connected via USB to one of the computers but its use is shared. Such a home network is often connected to the Internet by a combined DSL modem, firewall, and wireless access point. This environment is typical of Operational Environment D. However, one of the family members uses their laptop computer at home to connect to their employer's corporate network so that they can work at home on product launch plans for the aforementioned pharmaceutical company. The laptop, the wireless connection, and the HCD and its host computer would need to be able to operate as an Operational Environment A island within this typical Operational Environment D environment.

5. Hardcopy device assets

5.1 Overview

In this clause, HCD assets are defined and their relative importance in each operational environment is discussed.

5.2 HCD asset definitions

5.2.1 User Document Data

Minimally, the HCD processes User Document Data. User Document Data consists of all the information in the users' documents processed by the HCD, including the original hardcopy media being scanned or copied, electronic files to be printed, image data from scanning or fax, printed hardcopy output, and deliberately or residually stored data in hard disks or other memory devices.

5.2.2 User Function Data

Depending on the function and design of a particular device, an HCD may also have User Function Data. User Function Data consists of the information about the job that is to be processed. This information includes job instructions and job status.

5.2.3 HCD Protected Data

HCD Protected Data is information for which alteration by a user who is neither an administrator nor the owner of the data would have an adverse effect on the operational security of the HCD, but for which disclosure is acceptable. It may be stored in flash memory, on an HDD, or by using other means. Examples of HCD Protected Data include the following:

- a) HCD device job and usage logs, scan and fax address books, and device configuration
- b) Network management data such as IP addresses
- c) An HCD's digital resources and other resident data that is not necessarily part of User Document Data or HCD software such as fonts or stored forms

5.2.4 HCD Confidential Data

HCD Confidential Data is information for which either disclosure or alteration by a user who is neither an administrator nor the owner of the data would have an adverse effect on the operational security of the HCD. It may be stored in flash memory, on an HDD, or by using other means. Examples of HCD Confidential Data include the following:

- a) User and administrator passwords
- b) Device management data such as security event audit log data

5.2.5 HCD Physical Resources

An HCD's *physical resources* include components of the HCD and consumable items such as paper, ink, and toner.

5.2.6 HCD Availability

The ability to use the HCD can be considered an asset. In some operational environments, it is important to ensure that authorized users have timely access to the HCD. In other environments, it is important to prevent unauthorized users from using the HCD.

5.2.7 Software

The software that controls the function of the HCD is an asset that typically has two forms: *firmware* and *applets*.

5.2.7.1 Firmware

Firmware is any persistent instructions and data in the HCD that provides basic functions of the HCD, is developed by the manufacturer, is embedded in the device, and is infrequently updated.

5.2.7.2 Applets

Applets are HCD application software designed to be executed from within another application that provide additional capabilities for customer- or industry-specific purposes, sometimes developed by the customer or a third party, and possibly installed on demand.

5.2.8 External Environment

Although not part of the HCD itself, the External Environment consists of other IT equipment that is interconnected or interoperates with the HCD and can be threatened by certain kinds of exploits against the HCD. However, exploits against external IT devices that might threaten the HCD are beyond the scope of this standard.

5.3 Asset values in the operational environments

Based on the operational environment descriptions in Clause 4, Table 2 lists the relative value or importance of HCD asset categories in each of the environments:

Table 2—Asset values in each operational environment

Asset	User Document Data	User Function Data	HCD Protected Data	HCD Confidential Data	HCD Physical Resources	HCD Availability	Software	External Environment
Operational environment								
A	High	High	High	High	Low	Moderate	High	Moderate
B	Moderate	Moderate	Moderate	High	Moderate	Moderate	Moderate	Moderate
C	Low	Low	Moderate	High	High	High	Moderate	Moderate
D	Low	Low	Low	High	Moderate	Moderate	Low	Low