INFORMATION SECURITY

Proceedings of the IFIP TC11 Seventh International Conference on Information Security: Creating Confidence in Information Processing, IFIP/Sec '91
Brighton, UK, 15-17 May 1991

Edited by

DAVID T. LINDSAY
Digital Equipment Co. Ltd.
Newbury, UK

WYN L. PRICE
Formerly of the
National Physical Laboratory
Teddington, UK

1991

NORTH-HOLLAND

ELSEVIER SCIENCE PUBLISHERS B.V.
Sara Burgerhartstraat 25
P.O. Box 211, 1000 AE Amsterdam, The Netherlands

Distributors for the United States and Canada:
ELSEVIER SCIENCE PUBLISHING COMPANY INC.
655 Avenue of the Americas
New York, N.Y. 10010, U.S.A.

Library of Congress Cataloging-in-Publication Data

IFIP TC11 International Conference on Information Security: Creating Confidence in Information Processing (7th : 1991 : Brighton, England)
Information security : proceedings of the IFIP TC11 Seventh International Conference on Information Security--Creating Confidence in Information Processing, IFIP/Sec '91, Brighton, UK, 15-17 May 1991 / edited by David T. Lindsay, Wyn L. Price.
p. cm.
Includes bibliographical references.
ISBN 0-444-89219-2
1. Computer security--Congresses. 2. Data protection--Congresses.
I. Lindsay, David T. II. Price, W. L. III. Title.
QA76.9.A25I46 1991
005.8--dc20 91-30553
CIP

ISBN: 0 444 89219 2

PREFACE

The contents of this book are the papers presented at the IFIP/SEC'91 Seventh International Conference and Exhibition on Information Security, held in Brighton, United Kingdom, 15-17 May 1991, and organised under the auspices of the IFIP Technical Committee 11 with the cooperation of the British Computer Society and the EDP Auditors Association, European Region.

The theme of the Conference, "Creating Confidence in Information Processing" was particularly chosen because of the increasing world-wide growth in computer-related crimes and other threats to computer systems and the consequential concerns by users about the adequacy of the security of their systems.

The Conference, therefore, examined the criticial information security issues facing Society and through its distinguished international speakers presented technical as well as organisational solutions to these issues. Particular subjects discussed included Information Technology Security Evaluation Criteria (ITSEC), logical access control mechanisms, security management and awareness, applications and database security, EDI security, PC security and, not least, auditing and control aspects. Specific concerns about computer viruses and how to deal with them were reviewed, as well as, on a more general basis, how to investigate computer crime.

Attention was also given to legislative measures which are increasingly being adopted to provide additional protection of information against activities which can damage both individuals and organisations.

We warmly thank all those who participated in this Conference and in particular the members of the Organising Committee for their extensive contributions, the International Programme Committee members for their support, the speakers for their excellent presentations and, not least, the delegates whose active involvement ensured the success of this event. We would also like to thank those companies who generously supported the Conference and accompanying Exhibition, and Elsevier Seminars for their excellent administration.

David T. Lindsay
Chairman, Organising Committee

Wyn L. Price
Chairman, Programme Committee

COMMITTEES

ORGANIZING COMMITTEE

David T. Lindsay, Chairman
William Bound
Paul Evans
Mike Jones
Joe J. Kenny
William List
Ron A.J. Middleton
Penny Moon
Phil Phillips
Wyn L. Price
Karen Richardson
Gill Spear
Peta Walmisley
Duncan Whitley

INTERNATIONAL PROGRAMME COMMITTEE

EUROPE

Wyn L. Price, UK, Chairman
Klaus Dittrich, Switzerland
Andre Grissonanche, France
Per Hoving, Sweden
Knud Kristiansen, Denmark
David Lindsay, UK
Juhani Saari, Finland
Paul Williams, UK

NORTH AMERICA

Jim H. Finch, Canada
Peter P.C.H. Kingston, Canada
Martin Kratz, Canada
William H. Murray, USA

AUSTRALASIA

John Beatson, New Zealand
William Caelli, Australia

ACKNOWLEDGEMENTS

The IFIP/SEC'91 Organising Committee
wishes to thank

Digital Equipment Corporation
and
PC Security Ltd.

for their generous sponsorship and support
and the following for their cooperation

British Computer Society
EDPAA, European Region

TABLE OF CONTENTS

Information Security
D.T. Lindsay and W.L. Price (Eds.)
Elsevier Science Publishers B.V. (North-Holland)
1991 IFIP

Opening Address

H.J. Ivey

Head, Open Systems and IT Security Branch, Information Technology Division, Department of Trade and Industry, 151 Buckingham Palace Road, London SW1W 9SS, United Kingdom

Your Royal Highness, Lord Lieutenant, Madam Mayor, Chairman, Ladies and Gentlemen.

I am not, as you will have perceived, the Minister! Nevertheless I do know that Mr Leigh is most disappointed at not being able to be here with you today, and he has asked me to convey his regrets to you personally. The Minister needs to appear in debate at the House of Commons on Community legislation relating to fair contract terms, in his capacity of being not only Minister for Industry but also Consumer Affairs. I have been asked to outline what the Minister would have said.

The Minister would have been pleased to have been able to join with you today - a widely representative and international audience - on a subject of much importance in, for example, protection of company assets, trade, and, not least, the interests of the consumer.

The Department of Trade and Industry seeks to ensure that users and suppliers of information technology operate in a market environment which is competitive, innovative, free of unnecessary regulation, and sensitive to the interests of the consumer.

We see our rôle in information security as raising awareness of its importance, encouraging the development of appropriate standards, fostering innovation, and monitoring the impact of the legal framework.

On awareness, the Department has run a campaign for over a year now, targeted particularly at small and medium-sized enterprises, drawing to their attention steps they should consider to tighten security of their information systems. Already the campaign has a database of over 5,000 interested organisations, and is addressing an even wider audience through the media. As the campaign matures over the next two years, we aim to reach even wider audiences through "market influencers" such as suppliers, dealers, consultants and local industry associations.

On standards, we have played a pivotal role in helping to develop the evaluation process for products and systems. Jointly with the Communications-Electronics Security Group or CESG, based in Cheltenham, we have worked with our colleagues in France, Germany and the Netherlands to produce the harmonised "IT Security Evaluation Criteria", commonly known as "ITSEC". It is intended that ITSEC will be published this June for a trial period of two years. You will be hearing more about the criteria later today.

Just two weeks ago DTI announced the launch of a Scheme, to be run jointly by DTI and CESG, for evaluating products and systems against the criteria. The Scheme should lead to an increase in the availability of evaluated products, bringing benefits to both users and suppliers.

We are also actively supporting development of international standards. During the last two years, the DTI IT Security standards support programme has enabled UK industry and commerce to participate selectively in key items of security-related IT standards work. This includes assistance in the management and coordination of UK input to national and international standards programmes. We are now working closely with DISC, the new UK IT standards organisation within BSI.

On the legal framework, DTI gave active support to Michael Colvin, M P for Romsey and Waterside, when he piloted the Computer Misuse Bill through Parliament last year. Now we have the Computer Misuse Act. It falls to the Department to seek to ensure that industry and commerce are aware of the Act, that they take it fully into account in their IT security strategies and operational procedures, and that there are no impediments to their seeking prosecutions where appropriate. There is also, of course, the very considerable deterrent effect that the Act has already had, according to the views of IT security experts in the field.

There is no publicly accessible, centrally-held information on the incidence nationally of computer misuse. However, anecdotal evidence suggests that much computer misuse goes undetected, or if it is detected, computer users can have difficulty in collecting the necessary evidence that would link the misuse to an individual. The Act provides legal sanctions against offenders, but it naturally requires successful detection of the offence, and the careful collection of evidence, to bring a potentially successful prosecution.

To assist in furthering the effective operation of the Act, it seems desirable that both police forces and the business community should be able to refer to readily available, up-to-date advice to help in the detection and collection of evidence, and in the prosecution of misuse offences.

The Department therefore announces today the launch of a study to find out the particular needs both of the police, and of the business community, in their seeking to take full advantage of the Act. The study aims:

First — to identify and describe any requirements the police and the business community may have for expert advice on all aspects of computer misuse; and particularly in relation to operation of the Computer Misuse Act;

Second — to identify main sources of advice and expertise on computer misuse currently available to the police and to the business community in the UK, and whether developed in-house or 'bought in';

Third — to assess to what extent their needs are or could be met from currently available sources;

Fourth — to analyse the perceived requirement for provision of expert advice and, where appropriate, make recommendations on any new mechanism(s); and

Fifth — to report on the extent to which the police and the business community may be prepared themselves to resource any new mechanism(s) that are believed to be necessary.

The study will be carried out for the Department by Consultants. Work will begin immediately, and should be completed by September this year. A Press Release giving further details is being issued today.

In all our work, we are concerned that we should proceed in step with our international partners. This is fully reflected in our links with Europe in the development of the evaluation criteria, and the development of a European Community study programme in information security. It also extends to partners elsewhere, for example the United States, and at both public and private sector levels. We are conscious of the importance of the security of information systems to trading relationships, particularly with the increasing adoption of Electronic Data Interchange (EDI), and the secure relationships between parties that EDI requires.

During the course of the Conference you will be hearing in further detail about some of the work that DTI is supporting. You will also, of course, be hearing about much other valuable work being carried out both here in the UK and elsewhere. Information security is of increasing importance and significance to all of us. In conclusion, the Minister wishes you well in your deliberations over the next three days.

Information Security
D.T. Lindsay and W.L. Price (Eds.)
Elsevier Science Publishers B.V. (North-Holland)

Criteria, Evaluation and the International Environment: where have we been, where are we going?

Steven B. Lipner
Digital Equipment Corporation
Littleton, Massachusetts, USA

INTRODUCTION

This paper presents a few observations on trusted system evaluation criteria. It begins with a summary of the history of the U.S. criteria and the current state of the European criteria. It then discusses the impact of criteria on the vendors and users of commercial computer systems. After suggesting some guidelines for the developers of new criteria, it goes on to suggest a new direction that may better serve the purposes of vendor and user communities, though at the price of abandoning some long-held beliefs.

I should stress at the outset that this paper deals only with commercial computer systems and commercial applications (and with civil government computer applications that are indistinguishable from commercial ones). Defense and national security applications have their own unique attributes -- particularly the need to deal with labelled or classified information. After more than ten years of looking, I am convinced that the unique attributes having to do with labelled information are not required in the commercial and civil sector.

I would also offer the caveat that this paper reflects about twenty years of experience in computer security, the last ten gained while working in the employ of a commercial computer manufacturer. While it reflects early experience as a defense security researcher and many discussions with security evaluators, researchers, criteria developers, and most of all, would-be users of secure systems, it is clearly written from a vendor perspective and should be read in that light.

THE EVOLUTION OF EVALUATION

About ten years ago, the United States Department of Defense issued the directive establishing the Department of Defense Computer Security Center. The primary role of the Center was to establish and operate a program that would evaluate the security properties of commercial computer vendors' products. The theory underlying the Center was that