cigref

CLUB INFORMATIQUE DES GRANDES ENTREPRISES FRAN
21, avenue de Messine, 75008 Paris, tél. 256.94.00 poste 24.9

76 297

le 11.05.76

Rapport du Groupe de travail "Sécurité" pour le Groupe des Responsables de Politique Informatique

version provisoire

S O M M A I R E

1. Présentation de la grille d'analyse de sécurité d'un centre

2. Bibliographie

Etude Bibliographique Datamation (avril 1974)

Autres documents à consulter (Datamation octobre 1974 - février 1975)

Etude Sécurité IBM

(La bibliographie proposée sera complétée dans la version définitive du rapport).

1. Grille d'estimation de la sécurité d'un Centre de Traitement Informatique

Le groupe de travail restreint propose une méthodologie d'estimation de la sécurité d'un centre informatique en se basant sur les remarques suivantes

a) La recherche de sécurité concerne l'ensemble de la chaîne de traitement de l'information et pas seulement son maillon central qui est le traitement sur ordinateur. Très souvent, les traitements amont et aval sont négligés au point de vue sécurité par rapport à la partie traitement ordinateur.

b) La totalité des risques doit être examinée et pas seulement ceux qui apparaissent comme les plus significatifs.

Le groupe de travail a déduit de ces remarques la grille ci-après qui doit être réalisée et remplie d'une manière spécifique pour chaque centre.

Le groupe de travail a réflechi plus particulièrement à certaines étapes du traitement pour vérifier la facilité d'utilisation de la méthode proposée. Après la mise en oeuvre de cette méthode dans certaines Sociétés du CIGREF, un examen d'ensemble de la méthode pourrait être repris.

Etapes du traitement des données / Risques	Incendie A	Grève B	Panne du matériel C	Destruction des informations D	Secret et détournement des informations E	Communications (lignes et Poste) F	Niveau des effectifs G	Energie H	Sabotage I
Saisie 1									
Circulation des informations 2									
Traitements 3									
Documentation sur les traitements (analyse, programmation) 4									
Conditionnement 5									
Restitution des résultats 6									

2. Bibliographie

2.1 Etude bibliographique Datamation (avril 1974)

Les ouvrages particulièrement recommandés par le groupe de travail sont les suivants :

- Computer Security Handbook (D. HOYT)
  - . Analyse des risques et questionnaires de sécurité
  - . Manuel d'examen des problèmes de sécurité
  - . Les questionnaires sont orientés à l'usage de l'assureur et de l'auditeur.

- Security, Accuracy, and Privacy in Computer Systems (J. MARTIN)
  J. MARTIN propose une analyse des risques et un examen des solutions techniques (liste de contrôles des risques). Il s'intéresse à la sécurité physique et le confidentialité des données. Il propose des modèles de police d'assurance. C'est un ouvrage rédigé pour le Responsable Informatique plus que pour l'Auditeur.

Autres documents à consulter :

- Security Standards for Data Processing
  by S. WOOLDRIDGE, C. CORDER, and C. JOHNSON
  J. WILEY & SONS, Inc., 1973
- Computer Data Security
  by H. KATZAN
  Van NOSTRAND REINHOLD, Co., 1973
- Security and Privacy in Computer Systems
  by L. HOFFMAN
  John WILEY & SONS, Inc., 1973
- Security Procedures for Computer Systems
  by C. HEMPHILL and J. HEMPHILL
  Dow Jones-IRWIN, HOMEWOOD, III, 1973
- Computer Security Management
  by D. VAN TASSEL
  Prentice Hall, 1972
- SAFE - Security Audit and Field Evaluation
  by L. KRAUSS
  Firebrand, Krauss, E. Brunswick, N.J., 1972

Books

COMPUTER SECURITY— something old, something new

The pages that follow contain a vertical, in-depth review of current security publications. Bob Patrick, DATAMATION's Editorial Advisor, has reviewed eight recent volumes on the subject. Mr. Patrick is well versed for the task. In his years as a consultant he has conducted many installation audits, including audits for 12 commercial firms (one with 14 separate computer centers). He has been behind the wire of some of the U.S.'s most sensitive military installations, and worked for a large university during the 1970 riot season.

Security Standards for Data Processing
by S. Wooldridge, C. Corder, and C. Johnson
J. Wiley & Sons, Inc., 1973
186 pp. $14.95

According to the dust jacket, this book was written by an American now living in England, an itinerant Oxford graduate who has worked in Australia and Hong Kong and writes radio scripts, and a third author who is a pioneer of effective security in the data processing industry. Hilarity aside, this volume is a rather comprehensive introduction to the subject. It is rather readable, perhaps with due congratulations to the script writer, and is punctuated with a series of security happenings that go towards dispelling the attitude that "it can't happen here."

To its credit, the book starts out discussing risks, proposes a risk analysis, and indicates that some one person should be assigned the responsibility of worrying about security. The second group of chapters addresses the traditional security subjects of personnel, the physical installation, access controls, procedural controls over the input, the libraries, and the operations. A separate, rather weak chapter is devoted to fire detection and prevention, and another rather sparse one covers disaster recovery. Almost as an afterthought, a chapter on on-line systems is thrown in and the basic skeleton of a security audit is given.

While the first part of the book is rather readable and will serve well to introduce senior management to some of the problems of computer security, the last half of the book is a disappointment. In trying to be non-specific and to write a book that would work both in England and America, they left out all the details. To one schooled in security matters, their checklists serve as memory joggers and from one of their checklist questions a security aficionado could rattle off 15 or 20 specifics. However, to the unskilled reader, the checklists are too general to be much more than a basic education. The book is mistitled since only one short chapter talks about security standards and it's the weakest of the lot. Surprisingly there are 40 pages of appendices (about 20% of the volume), none of which is of particular value and some of which will seem almost ludicrous to any manager who has had his computer installed more than six months.

Although this volume is not particularly useful to the established dp manager, it might be very handy for the manager who has to do business with a corporate security officer drawn from a roster of retired policemen.

Computer Data Security
by H. Katzan
Van Nostrand Reinhold Co., 1973
213 pp. $11.95

Harry Katzan is a prolific writer having five other books to his credit dealing with the IBM 370 and related software. The dust jacket touts this book as a "must" for everyone. That's one of the problems with it. It tries to tell *all* about computer security. Unfortunately, all it tells is what Harry Katzan knows about computer security.

Katzan is well-read and the book is heavily footnoted with Babcock, Browne, Glaser, Hoffman, Lampson, Peters, Petersen, Turn, Van Tassel, Ware, Weissman, and Westin. However, judging from the content, it appears that Katzan's only contact with security is through his readings. The first 100 pages rush through a rather well done introduction to computers in general, and the System 360 in particular. The figures are very good and allow the seasoned reader to trace how tables, registers, pointers, and control blocks intersect to accomplish some end. The System 370 is also covered, along with virtual memory and some features of the GE 645 and Multics. While this is very good background, it's left up to the reader to understand how all this technical detail is related to security.

The fifth chapter, "Data Security Considerations in a Computer Environment," is freely drawn from Petersen and Turn and several IBM manuals. It stays at a conceptual level and the reader keeps wondering why he went through all the details of that hardware and software if he isn't going to get deeper into security details. The chapter on methodology is lifted directly from Lampson, Graham, and Denning. As before, the diagrams are excellent, but a reader looking for something practical that will help him in his day-to-day environment will find nothing here.

The book closes with an overview of IBM's Resource Security System (available from IBM as GH20-0967) and finally a little treatise on the principles of cryptography and data transformations.

The dust jacket prominently features a teleprinter and the casual purchaser might be misled to assume that this has something to do with the contents of the volume. While time-sharing is mentioned a time or two, and remote access is included, the dust jacket and the title are misleading.

This is a book in search of an audience. For the seasoned professional, the hundred or so pages devoted to computer concepts are unnecessary and the back half lacks sufficient detail to be interesting. To the uninitiated reader, the front half moves too fast and uses too much jargon to be easy reading, and the back half assumes he has mastered the first half.

Missing is any method of estimating risks, any mention of physical protection or operational considerations, and any note about personnel, systems, or procedures. All in all the inexperienced reader could be easily misled to think that computer security is totally a subject of hardware, software, and communications. Since it's obvious that Katzen can write and since his figures are very good, it's a shame he didn't choose his audience profile more carefully, narrow his scope, and write a book which would be a contribution to the field.

Security and Privacy in Computer Systems
by L. Hoffman
John Wiley & Sons, Inc., 1973
414 pp. $16.95

Here is another example of how stereotypes are misleading. This book is a compendium of 23 papers, 22 of which have been published elsewhere. It is put together by a university professor who has spent most of his life in the academic community. Thus it has all the makings of a dull course book that someone slapped together to comply with an academic requirement for one publication a year.

Nothing could be further from the truth. The 23 papers were carefully selected as the best of the security literature to date. With one or two exceptions, each one is a landmark paper exposing some new concept, drawing together what is now viewed as obvious, or proposing a technical solution to a pressing problem. Hoffman has assembled these papers, written a tasteful introduction to each of the seven chapters, and added an excellent pi

face to the whole collection.

Those of us who have worked on the security scene for many years will be familiar with most of the papers at least by reputation. They have been often cited and in many cases extensively quoted. Hoffman puts them in the proper light and lets each author speak for himself.

The position taken is that security and privacy are troubles of the times aggravated by the speed and flexibility of the modern computer. Hoffman notes that the problems are mainly political with some technical overtones. Each of the various authors attempts to take a positive attitude and protect the individual while searching for the economies that go with advanced technology.

While the manager of a dp installation won't find much in this volume to assist him in solving his day-to-day problems, this book should be required reading for all do-gooders, all self-appointed experts, all legislative staff men, and any who propose to address Congress or the state and local governments on matters related to security. Hoffman has done the field a service by collecting and tastefully presenting the landmark documents in the debate related to concepts, rights, and individual freedom.

Security Procedures for Computer Systems
by C. Hemphill and J. Hemphill
Dow Jones-Irwin, Homewood, Ill., 1973
246 pp. $11.95

The elder Hemphill has been an investigator and an FBI agent; he now works for a protection agency. The youneer Hemphill is a recent PhD in Electrical Engineering and is now in the Air Force. The preface indicates that this book is a nontechnical presentation for general business management. It does a pretty good job of being just that.

There is almost universal agreement among all authors that physical security is the foundation of all computer security plans. This book concentrates almost exclusively on that physical security. In its chatty style, liberally punctuated by reports of actual events, it treats natural disasters, fire, access control, man-made disasters, and disaster planning. However, the chapters on computer system backup, dp record storage, machine room procedures, remote access systems, and the like are as weak as the other chapters are strong.

The book is rather readable and is liberally sprinkled with quotes from the publications most dp managers don't read very often: *Administrative Management, Harvard Business Review, Best's Review, The Office, Nation's Business,* and *The Wall Street Journal.* The shallowness of the prose and the sources cited lead this reviewer to conclude that this book was intended for the nontechnical business manager who wished to have a slight acquaintance with computer security matters so he could name drop at the next board meeting. However, the book is not totally without interest to the computer professional. Some few of us will be building new facilities in the next few years. The chapters on physical security, if carefully read, would allow you to construct a bill of particulars to use in instructing the architect in planning your new facility.

The content of the book is superficial, but not misleading. The title is misleading for nowhere in the tome is a set of procedures enumerated. The content consists of narrative punctuated with descriptions of happenings, and each chapter is sealed off with a series of review questions much like the high school texts of 20 years ago. The book is concluded with a rather complete nine-page bibliography, drawn mostly from the nontechnical press. The student, the policy-maker, or the computer professional seeking case history material will find the bibliography of value.

Computer Security Handbook
by D. Hoyt
Macmillan, 1974
165 pp. $20.00

This book is a collection of 12 separate papers produced by the Computer Security Research Group, an outgrowth of several chapters of the Assn. for Systems Management in New York and New Jersey. Many of the articles were written by members of consulting houses and the others were written by employees on the corporate staffs of large industrial firms.

Each article is written in machine-independent form and most cover general concepts without getting too specific. They are not edited to a consistent format, nor do they contain a consistent level of detail. The first one, by A. E. Hutt, describes management's role in computer security. It is excellent and that excellence derives from a detailed risk analysis performed for the XYZ Company. After the risks are enumerated, the probability of occurrence is estimated, the range of the loss is estimated, and weighted risk values are computed. The results are then distilled to enumerate those with the highest maximum risk and distilled again to enumerate those with the highest weighted risks. The theme is: Avoid paranoia and soberly assess your exposure.

In the back of the book is an informative chapter by G. R. Migliaccio. He tells what the computer shop looks like from the insurance point of view and there is an extensive questionnaire used for performing an insurance risk survey which is enlightening if you read between the lines. All the papers in the book are aimed at the small to medium size installation. The DPMA member would feel comfortable with this book as would most corporate controllers in the $100 million per year gross class. The sample forms they supply, the short checklists that appear at the end of most chapters, and the diagrams used by the various authors all are directed to the installation which has a low level of computer and systems complexity.

As it stands, this is one of several books in the field that could be termed security primers. It would be useful in a college survey course, for legislative analysts who wonder what all the fire and smoke is about, for managers of small to medium size shops and their bosses, and perhaps for operations management in large facilities. Unfortunately, by making it machine-independent they left out most of the meat.

Computer Security Management
by D. Van Tassel
Prentice Hall, 1972
212 pp. $10.50

Van Tassel gets credit for being one of the first to attempt to cover the spectrum of security topics between two covers. His is an early book, completed in 1972, and is included here for the sake of completeness. As with many of these early publications, it's a sampler of topics of interest to the author. It lacks any quantified method for assessing the risks for the computer center, gives physical security short shrift, and proceeds hummingbird fashion through 8 pages on dp controls; auditing; various kinds of errors; 11 pages on software protection, copyrights and patents; 11 pages on cryptographic techniques (the author's interest); and a whole section on time-sharing, without ever discussing on-line data files. The coverage is spotty, the checklists are skimpy, and the document is in need of reorganization and update.

Most readers are turned off by examples that use IBM 1401s, 7080s, and 360/50s. The field has marched forward and Van Tassel was behind even in 1972. The dust jacket states that the author is an acknowledged expert in the field of computer security and further claims the book contains detailed

coverage of software protection. After reading the content, I conclude neither claim is true.

SAFE—Security Audit and Field Evaluation
by L. Krauss
Firebrand, Krauss, E. Brunswick, N.J., 1972
143 pp. $29.45

Although this book has been available almost two years, it warrants review at this time because it is a checklist. After only 16 pages of introductory material, Krauss launches into 118 pages of checklists interspersed with 118 blank pages of worksheets. He covers personnel, physical security, data, programs, documentation, operational aspects, backup, development, insurance, and continuing security programs. An appendix contains a 10-page list of good sample readings in security from the late '60s and early '70s.

The introduction claims that this checklist approach provides something between an inflexible formula and an expensive, completely custom-made security audit. For the subjects he covers, Krauss has done just that. However, at the present stage of development, security considerations are so pervasive and cut across so many facets of a computer installation that no existing checklist can be used like a recipe. Checklists will merely suffice to stimulate the memory of an experienced investigator so he can explore the topics suggested in appropriate detail for his installation.

Associated with the checklists are a rather mechanistic system of rating where each finding is given a numeric rating from zero to four. These ratings are written next to the checklist item, totaled at the bottom of the page, and numerically summarized in a table at the back of the handbook. All of these numbers tend to intrude into the audit process. No topic as complex as security can be reduced to numbers at such an early stage in its development. If the handbook were used as the author intended, it would be too easy for a security auditor to give such attention to the numerical ratings, assigned weights, and the actual numeric evaluation that he would forget to think. Thus it appears that the proper way to use the SAFE Handbook is to ignore all the ratings and numerical weights and use the questions to review the installation.

On the other hand, the questions presented are not given any codings to indicate whether a question is related only to installations having requirements for very intense security or to general practice. Thus back-to-back one can find questions having to do with polygraphs, urinalysis to detect drug addition, and more general topics such as checking references and dates on an employment application.

Still, Krauss has produced the best set of checklists available in the field today. The sections on personnel and physical facilities are so complete that one would need to be selective and delete some that did not apply before conducting an audit. The remaining sections touch on the important major considerations, but require expansion to get the required level of detail.

For instance, the section on data, programs, and documentation would require major extension if one were going to audit a large complex computer shop. The section on operations attempts to cover computer operations, control procedures within the computer facility, and data handling procedures related to the computer facility. While trying to cover this breadth in a few questions, he sometimes leaves gaping holes as exercises for the user (e.g., "Where a time-sharing system is used, rate the security and information safeguards to prevent access to programs and data files by other users"). While what he provides is good, a large installation with extensive complexity deriving from on-line access and resident data bases would have to extend this question set significantly to be able to perform an adequate audit.

If a person had a security manager; and if that security manager knew hardware, software, operations, procedures, applications programming, and management; and if that security manager had the inquiring investigative mind of a cop; he could take this SAFE Handbook and (in about a month) develop a customized list of questions suitable for a specific installation audit.

Security, Accuracy, and Privacy in Computer Systems
by J. Martin
Prentice Hall, 1974
619 pp. $19.95

This weighty tome tells all but the most dedicated reader everything he wants to know about security. It contains 448 pages of good readable prose and 172 pages of appendices. It is aimed at the broad-gauge computer professional who has enough knowledge of computer programming, operations, procedures, and management to feel fairly comfortable in any one of these areas. It is authored and edited by one man and he has used a consistent style and vocabulary. In addition, James Martin understands systems and can write about them with facility.

This volume is organized into 38 chapters in five major sections. In the first section Martin covers the nature of the problem and in the remaining four sections he covers the design of the computer system, its physical security, its administrative control, and the legal and social environment in which it is embedded. Each chapter closes with a short list of directed readings. The majority of the appendices are chapter summaries (outlines) but he supplements the chapter on auditing with an excellent 23-page checklist.

The main thrust of the book is toward the design of improved systems. He discusses the problems intelligently and then proceeds to enumerate principles and list the features a proper design should include. He does not give any attention to the retrofit of existing systems or to assessing what you've got (with the exception of the auditor's checklist).

Although he works for IBM, he does a creditable job of sticking to principles and not getting lost in IBM jargon. However, he occasionally does use IBM hardware or software when he needs an example. In addition to being an excellent book for the general reader, the IBM design engineers could benefit from a careful review of its contents since he does point out many flaws in the current product line with suitable grace.

This is not a primer, and while he is sensitive to social concerns, he does not dwell on them. For the system designer who is faced with a design problem today, I can heartily recommend this book and its engineering approach to current problems.

—Bob Patrick

2.2 Publication IBM sur les problèmes de sécurité

La philosophie d'IBM en matière de sécurité a été en particulier présentée au séminaire Data Security (Bruxelles 1975).

La documentation proposée ci-après correspond à un examen systèmatique du problème sécurité. La brochure "42 suggestions pour améliorer la sécurité" est particulièrement recommandée.

Extrait de Study Summary - Volume 2

In May of 1972, the International Business Machines Corporation announced the formation of four study sites for the purpose of gaining more information about data security and identifying user requirements in this vital subject. External study sites were the Massachusetts Institute of Technology, TRW Systems, Inc., and the Management Information Division of the State of Illinois. The internal study site was IBM's Federal Systems Division.

The findings of these sites are documented in the following IBM publications:

Data Security and Data Processing Volume 1
Introduction and Overview (G320-1370)

Data Security and Data Processing Volume 2
Study Summary (G320-1371)

Data Security and Data Processing Volume 3
Part 1 State of Illinois: Executive Overview (G320-1372)

Data Security and Data Processing Volume 3
Part 2 Study Results: State of Illinois (G320-1373)

Data Security and Data Processing Volume 4
Study Results: Massachusetts Institute of Technology (G320-1374)

Data Security and Data Processing Volume 5
Study Results: TRW Systems, Inc. (G320-1375)

Data Security and Data Processing Volume 6
Evaluations and Study Experiences: Resource Security System (G320-1376)

As stated at the outset of the project, these publications report independent findings of the study and do not necessarily represent IBM's views or opinions.