

Information Security Management: Global Challenges in the New Millennium

Gurpreet Dhillon
University of Nevada, Las Vegas, USA

IDEA GROUP PUBLISHING
Hershey • London • Melbourne • Singapore

Aquisitions Editor: Mehdi Khosrowpour
Managing Editor: Jan Travers
Development Editor: Michele Rossi
Copy Editor: Maria Boyer
Typesetter: Tamara Gillis
Cover Design: Deb Andree
Printed at: Sheridan Books

Published in the United States of America by
Idea Group Publishing
1331 E. Chocolate Avenue
Hershey PA 17033-1117
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@idea-group.com
Web site: <http://www.idea-group.com>

and in the United Kingdom by
Idea Group Publishing
3 Henrietta Street
Covent Garden
London WC2E 8LU
Tel: 44 20 7240 0856
Fax: 44 20 7379 3313
Web site: <http://www.eurospan.co.uk>

Copyright © 2001 by Idea Group Publishing. All rights reserved. No part of this book may be reproduced in any form or by any means, electronic or mechanical, including photocopying, without written permission from the publisher.

Library of Congress Cataloging-in-Publication Data

Information security management : global challenges in the new millennium / [edited by] Gurpreet Dhillon.

p. cm.

Includes bibliographical references and index.

ISBN 1-878289-78-0 (paper)

I. Computer security--Management. I. Title: Global challenges in the new millennium.
II. Dhillon, Gurpreet, 1963-

QA 76.9 .A25 I54154 2000
005.8--dc 21

00-050544

British Cataloguing in Publication Data

A Cataloguing in Publication record for this book is available from the British Library.

issue as “what is the hardest problem to solve?” Then the type of algorithm is examined (i.e., the integer factorization problem, the discrete logarithm problem modulo p , or the elliptic curve discrete logarithm). The details of this evaluation go beyond the scope of this article, but suffice it to say that the more time required to break an algorithm, the more secure the algorithm. The figure given for reasonably good security was a key length that required 10^{12} MIPS years to break (MIPS stands for Millions of Instructions Per Second). This number was considered to be approximately the amount of computing power on Earth, working for a considerable amount of time. According to Certicom, this level of security required a key size of 1,024 bits. Given the current legislative environment, this may not be possible.

Efficiency is based on three criteria: computational overhead, key size and bandwidth. Computational overhead is based on computer technology, which is growing at substantial rates. Therefore, organizations may need to review the capabilities of new technologies as they become available because these technologies will ease the computational burden. Key size is currently limited by United States law, but could be changing. Organizations will need to keep informed about legislative changes and react accordingly. Bandwidth is a continual problem on the Internet and is not limited just to security issues. Given this situation, organizations must keep in mind that bandwidth problems will be a factor to consider in implementing electronic business security.

As with many technology issues, an organization must determine if they should develop the security technology themselves or buy the technology. The business must be able to answer yes to the following question: “Does the organization possess the required knowledge and do they have enough skilled personnel to develop the technology in-house?” Small organizations will likely need to acquire the technology. They will probably need to develop a working partnership with one or more technology companies that can provide not only the security required, but also the support needed to maintain the technology. In addition the partner(s) could provide guidance in selecting the appropriate technologies.

When choosing a partner, the business should look at numerous factors including: experience in the e-business arena, industry experience, global presence, reliability and stability. These last two issues (reliability and stability) are very important because many startup businesses lack the capital and experience to stay in business over a long period of time.

As mentioned earlier, the U.S. government is trying to limit the encryption key length. Various governments around the world will want to regulate various aspects of e-business. This will include security because some governments will want to have the ability to monitor the activities occurring in e-business. The reasons for this monitoring activity are many. They include: tax revenue, national security secrets and illegal activities. Because e-business can span national borders, businesses will need to keep abreast of varying legal issues in the countries in which they do business.

We also need to consider the adoption issues: interoperability and organizational acceptance. Interoperability is important because the Internet covers a variety of organizations with differing brands of hardware and software. If a particular technology were not capable of running on several different systems and platforms, this would seriously limit its usability. A number of standards are emerging. One is the CORBA (Common Object Request Broker Architecture) specification. Other competing standards include DCOM (Distributed Component Object Model), XML (eXtensible Markup Language), SOAP (Simple Object Access Protocol), and others. Companies developing security technology