# SAFEGUARDING CRITICAL E-DOCUMENTS

## IMPLEMENTING A PROGRAM FOR SECURING CONFIDENTIAL INFORMATION ASSETS

Robert F. Smallwood

Foreword by Barclay T. Blair

# Safeguarding Critical E-Documents

# Safeguarding Critical E-Documents

## *Implementing a Program for Securing Confidential Information Assets*

**ROBERT F. SMALLWOOD**

WILEY
John Wiley & Sons, Inc.

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada.

Limit of Liability/Disclaimer of Warranty: While the publisher and author have used their best efforts in preparing this book, they make no representations or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Neither the publisher nor author shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

For general information on our other products and services or for technical support, please contact our Customer Care Department within the United States at (800) 762-2974, outside the United States at (317) 572-3993 or fax (317) 572-4002.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books. For more information about Wiley products, visit our web site at www.wiley.com.

***Library of Congress Cataloging-in-Publication Data:***
Smallwood, Robert F., 1959–
Safeguarding critical e-documents : implementing a program for securing confidential information assets / Robert F. Smallwood.
pages cm
Includes index.
ISBN 978-1-118-15908-8 (hardback); ISBN 978-1-118-28227-4 (ebk); ISBN 978-1-118-28281-6 (ebk); ISBN 978-1-118-28687-6 (ebk)
1. Computer security. 2. Document Management. 3. Electronic records. 4. Cyberspace–Security measures. I. Title.
QA76.9.A25S627 2012
005.8–dc23 2011048567

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

*For Araceli*

# Contents

**PART III** E-RECORDS CONSIDERATIONS

**PART IV** INFORMATION TECHNOLOGY CONSIDERATIONS

# Foreword

Today, yet another organization will be forced to admit that it has lost control of its information. The admission will be elicited by a court, a regulator, a reporter, or even a hacker. The company will admit that it has no clear understanding of what information it owns, where that information resides, or what value it has. Finally, it will admit that a fundamental lack of information oversight has put the company and its shareholders, customers, and partners at risk.

Worldwide, businesses and their clients are plagued by the effects of information mismanagement. Each year, they spend more on hardware and software to protect their data, but information security continues to be compromised. What's broken?

Let's start here.

Imagine a world where your chief privacy officer doesn't care about privacy. Where your chief operations officer thinks operations are someone else's problem. Or where your chief financial officer thinks that her job is managing spreadsheets, not money.

Welcome to the world of information management: a world where C-level executives—chief information officers (CIOs)—who, despite having the word *information* in their title, are not actually responsible for information. Most organizations have had chief information officers for at least two decades, and yet, most still cannot answer this question: "Who owns databases—those who maintain them or those who produce them?"

A question, which by the way, was raised in 1984 by *Modern Office Technology Magazine*.

The failure of institutions worldwide to clearly answer this question is at the root of the problems Robert Smallwood addresses here. It's not the CIO's fault; in fact, most CIOs are very clear about their role. Most view themselves more as chief *infrastructure* officers, stewards of the information *systems*; the people who keep the lights on but who do not generate the electricity; the owners of the storage tanks, pipes, and faucets, but not of the water itself. Pick your analogy.

Rather, fault lies with chief executive officers (CEOs) and boards, who have failed to understand that *information* governance (IG) lies at the heart of *corporate* governance; who fail to listen to the CIO when he talks about the real scope of his job; who are stuck in a different decade (even century) because they think the problem is about moving boxes of paper from facility to facility; and who, finally, have failed to adapt the CIO role, delegate the problem to another C-level executive, or create a new assignment.

This is the world that this book seeks to illuminate. And it couldn't be more timely.

In the book, Robert lays out a framework for understanding this problem, and a plan for dealing with the details—from strategy to software. Both elements are essential. We need to redefine the way we look at the information problem, which Robert helps us to do. But we also need a practical manual for active information governance, which he also provides in the form of authoritative and seasoned guidance.

The path to successful information governance is long. This book should help make your journey shorter and less painful. Safe travels!

Barclay T. Blair
Founder and President, ViaLumina Ltd.
www.vialumina.com

# Preface

*If you reveal your secrets to the wind, you should not blame the wind for revealing them to the trees.*

—Khalil Gibran, writer and artist (1883–1931)

*Electronic document security* has come to the forefront of the business and political world with the 2010 exposure of classified U.S. military documents by the website WikiLeaks and its founder Julian Assange. With the threat of more disclosures, and plenty of examples of leaked information in the corporate realm, organizations are scrambling to plug gaps in electronic document security to protect critical information assets.

Protecting confidential electronic documents (e-documents) goes far beyond protecting military secrets. In the private sector it means safeguarding blueprints, software, price lists, financial data, strategic plans, legal documents, personnel files, and other private corporate data, which have real economic implications. According to the U.S. Commerce Department, intellectual property (IP) theft has been estimated at more than $250 billion and costs over 750,000 jobs annually. The International Chamber of Commerce has estimated the global fiscal loss to intellectual property theft is more than $600 billion per year—and rising.

After reading this book you will know why any breach of internal information—even one like the WikiLeaks scandal—can be prevented by leveraging *information governance* (*IG*) policies and processes. Some IG technologies have been in existence for almost a decade, and implementing them can ensure that e-document and communications security measures are followed and enforced. These technologies are maturing and some are sophisticated enough to remotely control and monitor access to confidential documents, even after such documents leave the organization or an employee in possession of them is terminated. The following chapters provide key steps and insights for protecting critical e-documents and securing confidential information assets.

This book lays out the threats that may compromise the critical electronic documents of an enterprise across various types of computing applications, from e-mail and instant messaging (IM) to mobile and cloud computing to social networking; then it offers advice and solutions for countering these threats.

This book will assist CEOs, senior managers, CIOs, records managers, information technology (IT) managers, compliance and risk managers, and others involved in information governance, e-document security, records management, and e-records implementations to make intelligent, informed decisions. For those seeking to implement a program for securing confidential information assets, bulk pricing for the book and e-book are available. Contact: safeguard@electronic-records-management.com.

# Acknowledgments

I would like to thank Andy Han, Bud Porter-Roth, Barclay Blair, Bill Broddy, Charmaine Brooks, and Paula Lederman for their contributions to this book. Special thanks to Adi Ruppin for his time and unique insights.

# Safeguarding Critical E-Documents

PART I

# The Problem and Basic Tools

CHAPTER 1

# The Problem: Securing Confidential Electronic Documents

The element of surprise has accounted for more victories throughout history than any other tactic, according to Sun Tzu in *The Art of War*. In 1941, the United States military was surprised by the attack on Pearl Harbor and, as a result, would learn a valuable lesson about preparedness and vulnerability.[1]

## WikiLeaks: A Wake-Up Call

Today, attacks on organizations' information infrastructure occur daily, siphoning off confidential information. The most well-known cybersecurity breach is that associated with the WikiLeaks incident, in which confidential military, diplomatic, and corporate information was accessed and exposed online. This is perhaps the most visible example of an information security failure, but all types of organizations—not just the government and military—are at risk. And such breaches can be difficult to discover. Many times these types of incursions take place undetected for months, or even years, compromising the position of the victim organization and eroding the value of its information and stakeholder equity.

Since it is now widely known and accepted that the impact of leaked confidential information is real and the consequences are serious, organizations must constantly be on guard to protect confidential documents. There are specific steps that can be taken to counter the ongoing threat.

A number of countermeasure steps and processes that support information governance (IG) are available. These must be implemented alongside new technologies to enforce electronic document security (EDS). IG deals with the policies that control access to and use of information. They are a critical first step. For instance, in the case of WikiLeaks, a U.S. Army private allegedly provided classified military information to Julian Assange. A policy should have been in place to disallow low-level personnel from accessing the Secret Internet Protocol Router Network (SIPRNet), which is used to transmit classified information. Protecting confidential e-documents begins with robust and thorough policy analysis, starting with the questions "How are we going to govern the use of our confidential information? Who gets access to which information? Where? And when?"

> Ironically, the technology that could have secured documents and prevented them from leaking is used by WikiLeaks itself to control access.

Once these key questions are answered, newer EDS technologies can be applied to enforce the policies and control the access and use of information. Commercial and defense software providers have created systems that can safeguard electronic documents and records, wherever they may reside or be transported. The latest generation of this technology has advanced so that policy management is more streamlined and control over e-documents can occur remotely, anytime or anyplace, whether on a hard drive, thumb drive, mobile device, website, or in transit.

The goal of a program to secure confidential information assets is to provide complete document lifecycle security (DLS) for critical electronic documents and records, from their creation and use to their final archiving or destruction.

In 2010, the federal government took steps to better protect its information infrastructure by launching United States Cyber Command (CYBERCOM). The mission of the project is to "synchronize the Defense Department's various networks and cyberspace operations to better defend them against the onslaught of cyber attacks."[2] Unfortunately, it does little to address the issue of misuse of authorized data retrievals by insiders with security clearance. That is where clear and enforced IG, and technology tools, are critical to securing internal information assets.

> The goal of a program to secure confidential information assets is to provide complete document lifecycle security (DLS) for critical electronic documents and records, from their creation and use to their final archiving or destruction.

This book details the specific policies that need to be created for various information delivery platforms as well as the specific technologies that are needed to control, manage, and audit the use of electronic documents. These solutions are available; they simply take time, a focused effort, an adequate budget, and strong management resources to accomplish. And IG is not a one-off, one-time effort; once the program is in place, it must be consistently monitored, audited, and reviewed. *Leaving an organization vulnerable to data spills and breaches is due to poor management, and presents an avoidable business risk.* This risk can be avoided with proper policy analysis, planning, communication, and auditing as part of an overall IG program, and by leveraging security technologies.

## U.S. Government Attempts to Protect Intellectual Property

The theft of intellectual property (IP), which includes software source code, patented designs and blueprints, research, customer lists, and business methods, is a growing problem, and the U.S. government stepped in to combat it. In early 2010, the Department of Justice (DoJ) formed an IP task force to focus law enforcement efforts on the nettlesome and increasing problem of IP theft.[3]

The DoJ is trying to coordinate at multiple levels to streamline efforts between state, federal, and international law enforcement agencies to address IP theft, which has real economic consequences, especially for providers of software which is commonly illegally copied. Access to proprietary software source code must be securely monitored as it is a critical information asset for software development companies. The same is true of other providers of IP, such as law firms, consulting firms, advertising agencies, research companies, and the like.

## Threats Persist across the Pond: U.K. Companies on Guard

The problem of inappropriate or criminal access of confidential information assets spans the globe. In the United Kingdom, it was reported that cases involving employees taking confidential data from the workplace tripled from 2008 to 2009, and they have continued to increase today.[4]

Hard economic times may have contributed to the rise, as employees moved to new jobs or started new businesses using confidential information (e.g., client contact information) stolen from their previous employer. But many of these cases could have been prevented with proper IG polices and enforcement using EDS technologies.

## Increase in Corporate and Industrial Espionage

Corporate espionage is not new, and it has tangible costs. Ford is reported to have suffered a loss estimated at $50–$100 million as a result of the theft of confidential documents by one of its own employees. A former product engineer who had access to thousands of trade secret documents and designs sold them to a competing Chinese car manufacturer.

In another case of industrial espionage, the car manufacturer Renault filed a criminal complaint, asserting that another company tried to buy secrets related to its electric car program.[5] Several executives were ultimately suspended, showing that in our highly competitive business environment, ethics may be cast to the wayside if it means gaining an advantage—or, in the case of the complicit executives, financial gain. This can occur at the highest levels of enterprises, not just in the trenches.

Some schemes can be quite deceptive and devious, masked by standard operating procedures. Granting remote access to confidential information assets for key personnel is common. Granting medical leave is also common. But a deceptive and dishonest employee could feign a medical leave while downloading volumes of confidential information assets for a competitor—and that is exactly what happened at Accenture, a global consulting firm. During a fraudulent medical leave, an employee was allowed access to Accenture's Knowledge Exchange (KX), a detailed knowledge base containing previous proposals, expert reports, cost-estimating guidelines, and case studies. The employee went to work for a direct competitor and continued to download the confidential information from Accenture, estimated to be as many as 1,000 critical documents. While the online access to KX was secure, the use of the electronic documents could have been restricted even *after* the documents were downloaded, if newer technologies were deployed to secure them. Software security protections can be employed to seal the documents and control their use—even after they leave the organization.

> Ford's loss from stolen documents in a single case of IP theft was estimated at $50–$100 million.

Other recent high-profile industrial espionage and document leakage cases include:

- Hybrid car trade secrets were stolen from General Motors by an engineering employee in a scheme to sell them to rival Chinese car manufacturers.

- Huawei Technologies, the largest networking and mobile communications company in China, was sued by U.S.-based Motorola for allegedly conspiring to steal trade secrets through former Motorola employees.
- Health information of 1,600 cardiology patients at Texas Children's Hospital was compromised when a doctor's laptop was stolen. The information included personal and demographic information about the patients, including their names, dates of birth, diagnoses, and treatment histories.[6]
- Car burglars made off with personal records of 4,000 patients of a Portland, Oregon, psychologist and the names and Social Security numbers of 2,900 jobless residents in the county.
- MI6, the U.K. equivalent of the U.S. Central Intelligence Agency (CIA), learned that one of its agents in military intelligence attempted to sell confidential documents to the intelligence services of The Netherlands for £2 million GBP ($3 million USD).
- U.K. medics lost the personal records of nearly 12,000 National Health Service (NHS) patients in just eight months. Also, a hospital worker was suspended after it was discovered he had sent a file containing pay-slip details for *every* member of staff to his home e-mail account.[7]
- Personal information about more than 600 patients of the Fraser Health Authority in British Columbia, Canada, was stored on a laptop stolen from Burnaby General Hospital.

The list of breaches and espionage could go on and on, more than filling the pages of this book. It is clear that it is occurring and that it will continue. Safeguarding confidential information assets cannot rely solely on the trustworthiness of employees and basic security measures. It takes up-to-date information governance efforts and newer technology sets. Executives and senior managers can no longer avoid the issue, as it is abundantly clear that the threat is real and the costs of taking such avoidable risks can be high. A single security breach can cost the entire business.

## Risks of Medical Identity Theft

Rising medical identity theft is alarming and damaging to consumers and represents a liability for health care organizations. The U.S. government has become more involved, establishing the President's Task Force on Identity Theft and a medical-specific program in conjunction with the Office of the National Coordinator for Health Information Technology (ONC).[8] There are new initiatives and incentives for health care providers and institutions to automate health records. However, this move toward electronic patient records carries new medical identity theft risks. ONC commissioned