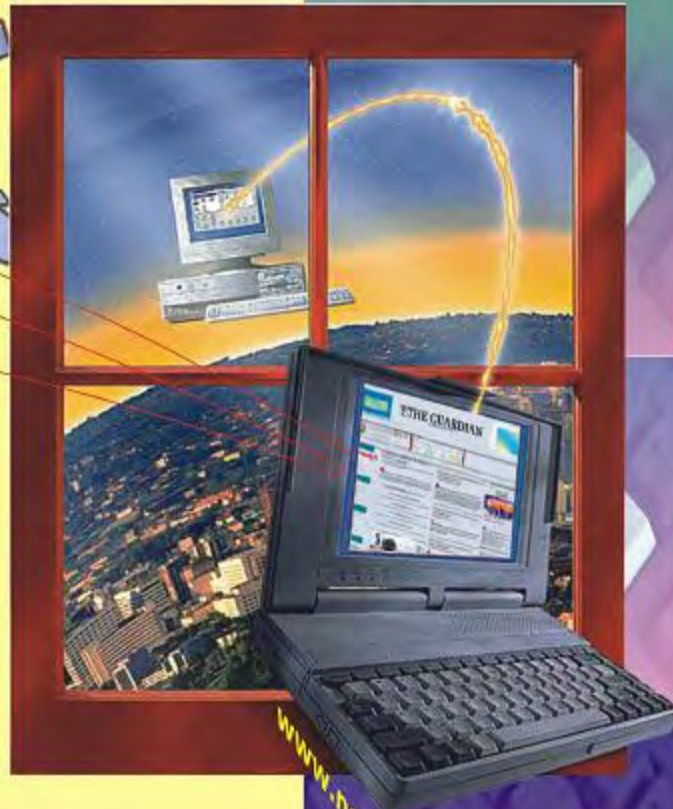


And the world keeps coming...



In July 2008,
Total Hits: over 18 million
Total Visits: over 1 million
Total Pages: over 4 million
worldwide



Read

THE GUARDIAN
online

www.ngrguardiannews.com

and get access to our
archives on past issues
and features.

Advertise your Products/Services and your Websites online



GUARDIAN NEWSPAPERS LIMITED

Rutam House, Apapa-Oshodi Expressway, Isolo,
P.M.B. 1217, Oshodi, Lagos.
Tel: 4931792, 4931799, 4525821, 2798269, 2798270
Fax: 4524080, 4931797; Advert Hotline: 7736351
e-mail: letters@ngrguardiannews.com

PLUS 7 COMPUTER SECURITY TIPS FOR STUDENTS



World
MAGAZINE

information management & security
www.inworldmagazine.rimsfoundation.org

The Official Magazine of

www.rimsfoundation.org



September/October 2008

Online Banking in Nigeria: **PROTECTING ONLINE TRANSACTIONS IN BANKS**

A Brief History of

**ENTERPRISE CONTENT
MANAGEMENT**

FOCUSED SOLUTIONS -

**IMPORTANCE OF
IDENTIFYING THE CORE ISSUES**

ALSO

- Managing Electronic Records
- Act Now To Prevent Data Breaches
- Information Security Fundamentals



UK £2 USA \$4 ₦500 Monthly

UK £12.5 USA \$25 ₦3,000 Annual Subscription



RIMA FOUNDATION wish to use this medium to thank those individuals and corporate organizations that supported the successful hosting of RIMAW 2008.

More grease to your elbow! We wish you success in all your endeavour and we look forward to seeing you next

year when we shall be organizing "RIMAW 2009 & RIMA Awards 2009"

Thank you!!!

Signed:

Oyedokun A. Oyewole
President

R I M A
FOUNDATION

IM Solutions

INFORMATION MANAGEMENT AND SECURITY CHALLENGES.

WE'RE THE SOLUTION.



Wolexdok Micro-Processor

(IT Support & Data Specialist)

Business Information Management & Security Solutions

Our partners

Please contact us for further information

Office: 3rd Floor, 1st Shedrach Building, 8, Association Avenue, Ilupeju Lagos State.

Annex: 74a, Palm Avenue, Mushin Lagos Nigeria. Tel: 01-8940451, 06023819008

Website: www.wolexdok.com Email: info@wolexdok.com, sales@wolexdok.com



IT Support & Data Specialist

CONTENTS

Cover Story

Online Banking in Nigeria:

PROTECTING ONLINE TRANSACTIONS IN BANKS

Page 14



Report

32

Disk Backup and EMC:
Addressing Today's Business Problems
The Changing Face of Data Protection



30 **Act now to PREVENT DATA BREACHES**

Reviews

10 **Managing Electronic Records**



36



37

Professional Training 

Features

34 **JOKES**

24

A Brief History of
ENTERPRISE CONTENT MANAGEMENT



Columns

6 **FOCUSSED SOLUTIONS - IMPORTANCE OF IDENTIFYING THE CORE ISSUES**

26 **Information Security Fundamentals**



Events

Records & Information Management Awareness Workshop & Exposition
28 August 2009
Sheraton Hotels, Ikeja Lagos

Records & Information Management Awards (RIMA Awards)
29 August 2009
Sheraton Hotels, Ikeja Lagos

Document Strategy Forum
10-12 September 2008
Hyatt Regency O'Hare, Chicago

Enterprise Architect Summit 2008
October 5-7, 2008
Arizona Grand Resort Phoenix, Arizona
(www.EASummit.com)

Storage Expo
15-16 October 2008
London, Olympia
(www.storage-expo.com)
tony.moyo@reedexpo.co.uk

ARMA International's 53rd Annual Conference & Expo
20-23 October 2008
Las Vegas October 20-23.

Business Continuity Expo
25-26 March 2009
Excel London
(www.businesscontinuityexpo.co.uk)

Infosecurity 2009
28 - 30 April, 2009
Earls Court, London

AIM Roadshow 2009
Edinburgh - Jun 1st
Leeds - Jun 2nd
Birmingham - Jun 3rd
Bristol - Jun 4th
London - Jun 5th

Professional Training

AIM is the community that provides education, research, and best practices to help organizations find, control, and optimize their information.

For over 60 years, AIM has been the leading non-profit organization focused on helping users to understand the challenges associated with managing documents, content, records, and business processes. AIM was founded in 1943 as the National Microfilm Association and later became the Association for Information and Image Management.

Today, AIM is international in scope, independent, and implementation-focused. As the industry's intermediary, AIM represents the entire industry - including users, suppliers, and the channel.

As a neutral and unbiased source of information, AIM serves the needs of its members and the industry through the following activities.

Market Education

AIM provides events and information services that help users specify, select, and deploy ECM solutions to solve organizational problems.

- Infonomics Magazine** (previously AIM E-DOC Magazine) - AIM's bi-monthly publication for over 37,000 subscribers. Each issue contains intelligent articles, case studies, thought-provoking columns, and lessons-learned.

- User Guides** - Thousands of office walls have been plastered with these graphic illustrations on ECM, Records Management, Compliance, Email Management, and more.

- AIM Wednesday Webinars** - Provide education on the key issues and trends affecting the industry and typically attract over 500 registrants per session.

- Focus On...** - Provide studies and white papers, articles and research studies focused on Compliance, Financial Services and Healthcare industry, Energy/Utilities, and Government.

Professional Development

AIM provides an educational roadmap for the industry.

- Certificate Training Programs** - Our industry leading Certificate Training Programs include enterprise content management (ECM), electronic records management (ERM), business process management (BPM), information organization & access (IOA/Search), enterprise 2.0 (E2.0), and email management (EMM). Courses are available via the web or classroom.

- AIM Expo and Conference** - The leading industry event for Enterprise Content & Document Management, which encompasses all the technologies that are used to capture, manage, share, and store documents and digital content.

- ECM Solutions Seminar** - General and vertically focused educational Seminars held in 20 cities throughout the

Markets Place

U.S. and Canada, help educate professionals with information on the latest industry trends, key business drivers, case study examples, solutions, and more.

- IM Expo** - The major educational event for the ECM industry, held in five or six locations each year across the United Kingdom.

- Info Ireland** - A two-day educational event held annually in Dublin Ireland.

Peer Networking

AIM creates opportunities that allow users, suppliers, consultants, and the channel to engage and connect with one another - through chapters, networking groups, programs, partnerships, and the Web.

- AIM Chapters** - A network of 39 chapters in North America providing educational and networking opportunities at the local level for AIM members.

- Communities** - groups of members and constituents that form or become their own communities.

Industry Advocacy

AIM acts as the voice of the ECM industry in key standards organizations, with the media, and with government decision-makers.

- Market Intelligence** - Industry research reports provide intelligent information about user trends and perceptions several times a year.

AIM Standards - AIM is an ANSI (American National Standards Institute) accredited standards development organization. AIM also holds the Secretariat for the ISO (International Organization for Standardization) committee focused on Information Management Compliance issues, TC 171.

Membership

Through year-round support, AIM offers several types of membership to suit your needs. Select the one that's best for you, and become a recognized leader in the ECM industry. Increase visibility for your company, develop standards for the industry, get industry information and research, and network with industry professionals and peers.

- Professional Membership** (for people using ECM products and services) Education, industry research, toolkits, awards, committees, and discounts.

- Trade and Advisory Trade Membership** (for suppliers of ECM products and services) Comprehensive market exposure and increased visibility for your company, products, and services.

- Document Management Service Provider Membership** (for VARs, VADs, systems integrators, and consultants) Specialized training and education, company visibility, annual forum, and networking.

Data Management Companies



Company name: VIALECT Inc
Address: 1435 Tecumseh Rd East Windsor, Ontario N8W 1C2
Tel: 519-258-2555
Toll free: 877-842-5328 (US and Canada)
Fax: 519-258-3563
Email: information@vialect.com
Website: www.vialect.ca

VIALECT RELEASES NOODLE!

VIALECT, a leading provider of business collaboration & social-networking software, announced today the release of **Noodle**. **Noodle**, formerly known as IntraNet, is now the flagship product of VIALECT.

Use your Noodle!
 "The name change is a result of product evolution" says founder Tim Dorey. "Companies are using our product for much more than just an intranet. Wikis and Blogs are being created, and with the latest version, Social Networks can now be built inside **Noodle**."

What's your corporate wisdom?
 One of the most exciting new features added is the Corporate Wisdom feature. Many collaboration and intranet projects fail due to inactivity. This inactivity is the result of outdated information, hard to use tools and employees not being encouraged to review and contribute to the overall success of the project. **Noodle** solves this problem by monitoring the Corporate Wisdom of each employee.

Corporate Wisdom is calculated by the total amount of items an employee reviews and the total amount of items the employee creates. These numbers are then added together and compared to the total site content to produce that user's Corporate Wisdom "rating". Corporate Wisdom also fluctuates as new content is added to the site.

Find people with expertise
 Also new with **Noodle** is the enhanced People section that displays the names and photos of all site members. This page has four different views so users can sort people based on group, expertise, status update and wisdom level.

What are you working on?
 Another new enhancement is the social-networking feature, What are you working on?. Each user can update their status and notify coworkers what they are currently working on. These updates can then be shared with fellow team members to facilitate corporate unity.

Deployment Options
Noodle is available in both an online service (SaaS) or a local software installation. **Noodle** can be installed on both Windows and Linux, and supports Microsoft SQL, Oracle and PostgreSQL databases. Free demos are available from the VIALECT website.

VIALECT will be launching **Noodle** at the **EMWorld & Intranets Conference** in San Jose, California on September 23. Demonstrations of the new Corporate Social-Networking features will be presented at Booth 234 at the show. For more information, or a trial version of **Noodle**, visit www.vialect.com.

About VIALECT
 VIALECT's mission is to help corporations improve productivity and achieve business objectives using social-networking tools. Our software creates a network based on participation, where users are the driving force. The product offers a suite of collaborative applications that are quick to set up, easy to use and extremely cost effective. VIALECT's ikt-centric software is designed for any organization that wants to accelerate team communications, better enable knowledge sharing, foster collaboration, and build online communities.

To find out more or create a free 30-day trial of **Noodle** visit www.vialect.com



Company name: Phoenix Technologies Ltd
Address: 915 Murphy Ranch Road Milpitas, CA 95035
Tel: 1-408-570-1000
Toll Free: 1-800-677-7305
Fax: 1-408-570-1001
Email: Haley.Couch@beinsync.com
Website: www.beinsync.com

About the Company

Phoenix Technologies builds world-class core systems software platforms, tools and applications that take full advantage of our history of expertise at the core of digital devices, to enable the broadest set of users a more simple, trusted and reliable experience.

Phoenix is dedicated to providing superior core systems software and platform software products for specifiers of connected digital devices. Phoenix enables OEM and ODM customers to differentiate and create value for their end users by dramatically improving the manageability, reliability and usability of their products. Phoenix's latest advancements in core systems software have led to the creation of a wide range of products that address the PC industry need for radically simplified and trusted computing.

Founded in 1979, Phoenix Technologies core systems software helped launch the PC industry more than 20 years ago. Today, we have extended this leadership beyond the PC to a wide range of platforms and other digital devices. Approximately 400 employees around the globe join in Phoenix's continual commitment to redefining core systems software and leveraging a history of expertise at the core of all digital devices to deliver the world's best core systems software products. Headquartered in Milpitas, California, Phoenix is traded on the Nasdaq National Market under the symbol **PIEC**.

Products

BeInSync offers powerful data solutions for individuals, professionals and businesses. These solutions allow users to have their data where and when they need it, by providing integrated online backup, PC synchronization, secure file sharing and remote file access. So, rather than install and run many different applications or run dedicated servers BeInSync gives you a one-stop solution that's simple, secure and affordable.

Businesses

Designed for businesses who would like to deploy and centrally manage the BeInSync solution for multiple employees.

Professionals

Designed for individual mobile professionals who'd like to use BeInSync to protect their documents, sync their home, office and notebook computers, and work together with partners or colleagues.

Training

RIMA Foundation Quarterly Training Program on Records & Information Management
 17 Jan. 2009

RIMA Foundation Quarterly Training Program on Records & Information Management
 13 March 2008

AIIM Professional Training Programme, (Practitioner, Specialist, Master) Certificate
 24th-27th March, 2009
 PROTEA HOTEL, Ikeja, Lagos State, Nigeria, West Africa.

AIIM Professional Training Programme, (Practitioner, Specialist, Master) Certificate
 24th-27th August, 2009
 PROTEA HOTEL, Ikeja, Lagos State, Nigeria, West Africa.

TechMentor
 7-10 September 2008
 New York
 (www.techmentorevents.com)

Visual Studio Live (VSLive)
 7-10 September 2008
 New York

Visual Studio Live (VSLive)
 13-16 October 2008
 Las Vegas

TechMentor
 13-16 October 2008
 Las Vegas
 (www.techmentorevents.com)

Visual Studio Live (VSLive)
 7-10 December 2008
 Dallas

From the Editor



'RIMAW 2008'... a success

It is worth note that the annual event put together by RIMA Foundation, Records and information Management Awareness Workshop, Awards and Exposition (RIMAW 2008) has come and gone, leaving behind the wonderful memories which can not just be forgotten in a hurry.

This year's event witnessed a wonderful array of quality guests and facilitators from top executives in the IT, Business and Banking sectors, and the number of Attendees this year was encouraging.

RIMAW Awards 2008 had the introduction of additional Awards from the usual eleven (11) to twenty five (25) categories, following our response to some of the feedback we got after last year's event, RIMAW 2007 which took place in Eko Hotels & Suite, Lagos.

May I used this opportunity to thank those who made RIMAW 2008 a success and assure participants that we have noted their comments and promise to improve on those areas mentioned.

Finally, I would like to CONGRATULATE the 2008 RIMA Awards' winners and also thank those corporate organisations and individuals who graced the event, we look forward to seeing you next year!!!

Thank you

Editor in Chief
 Oyedokun A. Oyewole
 President@rimaw.org

Don't miss the president's article every Friday in Guardian Newspaper (Executive Brief)



PUBLISHER RIMA Foundation

EDITORIAL
 EDITOR IN CHIEF
 Oyedokun A. Oyewole

SENIOR EDITOR
 Maduri S. Ugochi

ASSISTANT EDITOR
 Adegboye Arowojaye

TECHNOLOGY EDITOR
 Babo Josin

COPY EDITOR
 Nonye Emodu

CONTRIBUTOR
 Adeniran H. Adesina

DESIGN
 DIRECTOR, ART AND DESIGN
 Salami M. Toyin
 ART DIRECTOR
 Idowu Yakub

PRODUCTION
 PRODUCTION MANAGER
 Akintola S. Tawo

ASSOCIATE PRODUCTION ASSISTANTS
 Niyi Ayinde
 Adegboye Adeseye

RESEARCH
 RESEARCH MANAGER
 Oyedokun A. Oyewole

MARKETING
 DIRECTOR, MARKETING COMM.
 Ugochi S. Maduab

AASTY Media
 E-mail: aastymedia@rimaw.org
 © RIMA Foundation



RIMA Foundation

Office: 3rd Floor, 1st Shebarch Building, 8 Association Avenue, Ikeja Lagos State. Tel: +234-1-6940451, +234-8023819008

For Subscription Services and Enquiry, log on to:

<http://www.worldmagazine.rimafoundation.org>

E-mail: subscription@rimaw.org

Telephone Enquiry: 02-6940451, 08023819008

World Magazine is published monthly by RIMA Foundation, 8 Association Avenue, Ikeja Lagos State, phone +234-1-6940451, +234-8023819008, +234-02023819008. Annual subscription rates: United States - \$20, United Kingdom - £10, other foreign distribution - \$20, Local - \$10. Single copy price: United States - \$4, United Kingdom - £2, other foreign distribution - \$4, Local - \$2. Please include check or money order payable to RIMA Foundation with your order. All rights reserved. This content Copyright © 2008 RIMA Foundation. No part of this publication may be reproduced or transmitted in any form, or by any means, without permission in writing from the publisher.

Printed by: AASTY Media Ltd.
 Tel: 01-7437344, 08037129690



Samuel Okoro

FOCUSED SOLUTIONS - IMPORTANCE OF IDENTIFYING THE CORE ISSUES

Over ten years, when I was in charge of automation and instrumentation in a large brewing plant, a modern, PLC bottling line was installed.

Not quite long, we began to experience series of apparently isolated and seemingly random problems on the filler/crowner (the machine that fills and caps the bottle) on a weekly basis.

At one time, the bottles would come out half filled. At another, there would be missing caps or the water spray meant to drive, would fail to activate or CO2 pressure in the ring tank would fall below what was required to maintain smooth beer flow and the tank would be filled with foam. And so on.

Looking at these as a separate problems we spent hours tracing the cause of each problem and eliminating it (temporarily, it usually turned out).

However, another problem re-appear in its place, while battling to solve the one at hand each the day would wear on and finally sometime in the afternoon the problems would disappear as inexplicably as they had appeared and there would be stabilization of production throughout the week.

Unfortunately, these problems resurfaced the following week. The root of it was discovered to have emerge from the cleaning operation. The line was usually cleaned with powerful spray hoses. The electrical and instrumentation panel controlling the filler/crowner was located right beside the machine. it was not tightly sealed (faulty initial installation) and cleaning water sprays found its way into it, thereby creating random short circuits in the panel that resulted in unpredictable machine behaviour.

Identifying this core issue and remedying it solved the problem for good.

Some years later, another machine - the labeller began to exhibit series of random malfunctions involving the label magazine, glue pump and other components. But we had learned. Rather than waste time pursuing each separately, we tried to understand what was common to all of them. It was discovered that lubricating oil had found its way into the encoder, which controlled the timing of nearly all the functions in the machine.



Name: Alan Calder

Designation: Chief Executive

Organisation: IT Governance Limited

Alan Calder is a leading author on IT governance and information security issues. He is chief executive of IT Governance Limited, the one-stop-shop for books, tools, training and consultancy on governance, risk management and compliance.

Alan is an international authority on information security management and on ISO27001 (formerly BS7799), the international security standard, about which he wrote with colleague Steve Watkins the definitive compliance guide,

'IT Governance: A Manager's Guide to Data Security and BS7799/ISO17799'. This work is based on his experience of leading the world's first successful implementation of BS7799 (with the 4th edition published in May 2008) and is the basis for the UK Open University's postgraduate course on information security.

Other books written by Alan include 'The Case for ISO27001' and 'ISO27001 Nine Steps to Success', as well as several pocket guides in this series.

Alan is a frequent media commentator on information security and IT governance issues, and has contributed articles and expert comment to a wide range of trade, national and online news outlets. ■



DELETE YOUR VIRUS NOW!

Girl Friends Are Like Virus

They enter your life,
Scan your pockets,
Transfer your money,
Edit your mind,
Download their problems and
Delete your smile
So please get a wife (anti-virus)
to scare(scan) them away
before they break your heart-
disk

Get Rid Of W-O-R-K!

There is a dangerous virus being passed around electronically, orally, and by hand. This virus is called **Worm-Overload-Recreational-Killer (WORK)**.

If you receive WORK from any of your colleagues, your boss, or anyone else via any means DO NOT TOUCH IT. This virus will wipe out your private life completely.

If you should come into contact with WORK put your jacket on and take two good friends to the nearest grocery store. Purchase the antidote known as Work-Isolating-Neutralizer-Extract (WINE) or Bothersome-Employer-Elimination-Rebooter (BEER). Take the antidote repeatedly until WORK has been completely eliminated from your system.

By: Olatuji

Problem with Installation

I tried running Girlfriend 2.0 with Girlfriend 1.0 still installed, they tried using the same I/O port and conflicted. Then I tried to uninstall Girlfriend 1.0 but it didn't have an uninstall program. I tried to uninstall it by hand, but it put files in my system directory.

Another thing that sucks -- in all versions of Girlfriend that I've used is that it is totally "object orientated" and only supports hardware with gold plated contacts.

***** BUG WARNING *****

Wife 1.0 has an undocumented bug. If you try to install Mistress 1.1 before uninstalling Wife 1.0, Wife 1.0 will delete MSMoney files before doing the uninstall itself. Then Mistress 1.1 will refuse to install, claiming insufficient resources...What do I do?

Also, in this case, identifying the core issue and remedying it solved the problem for good.

The two real examples above provide a lesson that can be generalized to all systems: whenever several problems are occurring at the same time, no matter how seemingly unrelated the problems are, they are usually caused by a single, or at most a very few core issues. This statement applies, no matter the type of system and its complexity.

It thus makes sense that in attempting to improve on any system, the first thing to do would be to look beyond the problems and ferret out their causes. In TOC parlance, you should identify the system's constraint.

To do this, requires understanding the interrelationships between the various parts of the system. For example we would have found our solution earlier if we had understood the system and not just the machine that also the cleaning operation that was carried out.

The above conclusion applies when the area of interest is the whole organization, or a whole industry or supply chain, or even a whole economy. The proliferation of problems usually suggests one or a very few issues at their core.

How great is the impact of focusing on effort of core problems have on the effectiveness of solutions applied?

An electronics company in the US designed an experiment to answer this question scientifically. On their twenty one production plants, they implemented only "Lean" solutions in four plants and only "Six Sigma" solutions in eleven plants. In the remaining six plants, they implemented "Theory of Constraints" solutions (for focusing) in combination with "Lean" and "Six Sigma" (for solving problems in the areas of focus). What were the results like?

In all cases, they were able to reduce cost. The four "Lean" plants contributed 4% of the total savings achieved - about 1% per plant. The eleven "Six Sigma" plants contributed 7% of the total cost savings - less than 1% per plant. The last six plants that used TOC for identifying focus areas contributed 89% of the total cost savings. This is about 15% per plant! Which signifies the need for proper channeling of resource in the right areas for improvement.

=====

Samuel J. Okoro
LeapfrogAlliance Ltd
www.leapfrogalliance.com
+234 1 850 8180
+234 803 629 6415

Total Protection Security

SPYWARE IS THE DISEASE. WE'RE THE CURE.

Ever feel like you're being watched? Right now spyware on your computer could be watching your every digital move. Unless you have McAfee. More than just anti-virus protection, McAfee offers continuous security from spyware, hackers, and other threats to you and your family. Learn about our complete range of total protection solutions at McAfee.com

McAfee

McAfee, Inc. 3965 Freedom Circle, Santa Clara, CA 95054; 888.917.8765; www.mcafee.com. McAfee is a registered trademark of McAfee, Inc., and/or its affiliates in the US and/or other countries. McAfee Red in connection with security is distinctive of McAfee brand products. © 2008 McAfee, Inc. All rights reserved.

- The difficulties involved in efficient sharing or re-use of corporate information assets due to competing standards or the lack of a common data repository.

- Training end-users on multiple solutions is consuming precious IT and business resources.

- The high price tags associated with the purchase and operation of different solutions.

ESG's View

In today's IT environment, data and applications abound. An integrated data protection ecosystem has the potential to provide organizations with a level of efficiency and reliability they never dreamed of. Instead of managing multiple applications from multiple vendors, organizations manage multiple applications from a single GUI. Doing so has the immediate benefit of simplification and cost control, but has the long term potential to change IT and business dynamics all together. Today, revenue loss is typically calculated in time lost (in trying to recover data quickly and completely in recovery situations). What about lost opportunities? While organizations stand to lose potentially hundreds of thousands, if not millions, of dollars by not protecting data resources adequately, they

leave significant dollars on the table by not fully leveraging the data assets (or information) they already have. An integrated data protection platform can help organizations better leverage this information. By providing a continuum of data protection solutions and integrating them, EMC not only helps ensure that organizations have the right data protection tools for the right data at the right time which has a range of benefits as described in this report but puts organizations in a better position to maximize the value of the data assets it protects.

About

Enterprise Strategy Group (ESG) is a leading industry analyst firm that provides strategic guidance and unmatched service to technology vendors, IT professionals, venture capitalists, and institutional investors. The Enterprise Strategy Group evolved from the Enterprise Storage Group, and now offers products and services focused on application infrastructure and information security while it continues to set the tone for storage and information management. Enterprise Strategy Group sets itself apart from legacy analyst firms and boutiques by continuing to build its excellent reputation of assisting clients to make strategic business and IT decisions.

News

Paperless Boarding Pass Pilot

Source from Innovation & Technology
October 23, 2008



The electronic boarding pass pilot enables passengers to download their boarding pass on their cell phones or personal digital assistants (PDAs). This innovative approach streamlines the customer experience while heightening the ability to detect fraudulent boarding passes. Each paperless boarding pass is displayed as an encrypted two-dimensional bar code along with passenger and flight information. TSA security officers use hand-held scanners to validate the authenticity of the boarding pass at the checkpoint.

Ten airports are piloting this technology: Houston George Bush Intercontinental Airport (IAH), Ronald Reagan Washington National Airport (DCA), Newark Liberty International Airport (EWR), Logan International Airport (BOS), Austin-Bergstrom International Airport (AUS), San Antonio International Airport (SAT), Indianapolis International Airport (IND) and LaGuardia Airport (LGA) in New York, Seattle-Tacoma International Airport (SEA), and Cleveland Hopkins Airport (CLE).

Once the hand-held scanners are deployed nationwide, TSA will also use this technology to track wait times using standardized automated data collected at checkpoints. This development is expected to happen within about a year. ■



Disk Backup and EMC:

Addressing Today's Business Problems

The Changing Face of Data Protection

by ESG Enterprise Strategy Group

Continued from last edition

Integrated Data Protection Ecosystem

Clearly, implementing a data protection ecosystem is a good thing, but implementing an ecosystem of integrated applications can be even better.

Integrated platforms give users the flexibility to cover more or even all data protection bases from a single source. This contrasts with "point product" approaches in which multiple technologies (typically from multiple vendors) are used in combination to meet data protection requirements. The problem with a point product approach is that there is generally very little integration between applications. This can make management difficult (because multiple GUIs are needed to manage multiple data protection applications), increase CAPEX and OPEX costs (again because of the multiple applications required) and, importantly, make the data protection process a lot less fluid. Again, the idea behind the data protection ecosystem is

being able to apply the right data protection technologies to the right data at the right time and at the right price point throughout the data life-cycle. This requires a level of communication between participating data protection applications. The idea behind integrated platforms is to enable users to initiate and manage multiple data protection processes (e.g., volume snapshots, continuous data capture, replication, and even data de-duplication) from a single console. Of course, the level of benefit an organization will see from an integrated vs. a point product approach will vary, depending on the types and granularity of the data protection applications offered (e.g., replication, CDP, snapshot, VTL, data de-duplication, etc.) and how tightly the products are integrated. ESG contends that vendors that integrate these applications on the front-end and provide easily accessible and searchable secondary storage pool

options on the back-end will have a clear advantage in the market (see Sidebar: Keeping It Simple).

ESG Research¹ finds that this type of platform resonates with users. In fact, 62% of respondents of a recent ESG survey said they were interested in a more unified approach to data archiving. While this survey was specific to the digital archiving space, it is indicative of a general trend in the industry toward a more streamlined approach to data management due to the various technical, operational and financial challenges that result as IT environments become more diverse and complex. Such as:

¹ ESG Research Report: *Digital Archiving: End-User Survey & Market Forecast 2006-2010*, March, 2006.

- Evaluating, purchasing, implementing and managing an increasing number of discrete point products.

"It's the compliance that counts, not the badge on the wall"

Executives who claim that their organizations comply with ISO27001 but that they see no need to go through the bureaucracy of getting the 'badge on the wall' are only deceiving themselves. The reality, I suspect, is that most of organizations that won't submit their Information Security Management Systems (ISMS) to an external audit against ISO 27001 fear that, when it comes to the push, their systems would fail the test.

Survey after survey reveals a depressingly familiar information insecurity story. The 10th annual CSI/FBI survey revealed that, amongst the security-conscious, information security control-focused members of the CSI, computer crime continued to have a significant financial impact. The average incident cost \$204,000, and the top two security breaches were through virus attacks and unauthorized access both of which are comprehensively controlled through the controls and management systems mandated by ISO 27001. I am prepared to be that few, if any, of the CSI members who were victims of those attacks either hold a current ISO27001 certificate or are planning to pursue ISO27001 certification.

This evidence, combined with the findings of a recent survey carried out amongst UK-based organizations with ISO27001, suggests somewhat contradictorily that securing information is rarely the primary driver for achieving certification. The top reason was commercial advantage, summed up by one respondent who said that a certificate 'gives customers confidence that our data security is well managed and certified by an independent source.'

And it's that certification 'by an independent source' which is the real benefit of pursuing ISO 27001 in the first place. US regulators implicitly recognized the importance of external validation for information security effectiveness when they observed that: 'the best way to strengthen US information security is to treat it as a corporate governance issue that requires the attention of boards and CEOs.'

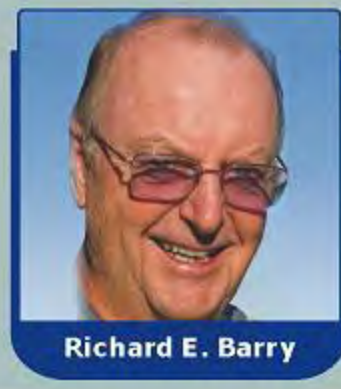
There are sectors in which the 'badge on the wall' debate is already history, and in which certification is

now becoming a basic business requirement. UK cheque printers, for instance, are required to comply with a sectoral version of ISO27001 and suppliers hoping to connect to the new NHS backbone are expected to comply with controls in ISO27001. Business Process Outsourcing companies are finding it much simpler to provide a copy of their ISO27001 certificate in their tender documentation than to answer detailed information security questionnaires.

Some of this might be expected: ISO27001 is originally a British Standard, and the UK government's Cabinet Office has, for several years, driven take-up across the UK public sector. And as more and more local authorities and public-sector organizations become certified, so the pressure for their private-sector suppliers to achieve the standard will increase and today's early adopters are clearly stealing a march on their competitors.

Information security management system certification can also be a short cut to best-practice compliance with a wide range of data compliance and regulatory requirements, ranging from Data Protection Acts across the EU, privacy and breach legislation across the OECD, and specific legislation such as GLBA, HIPAA and Sarbanes Oxley. Determined outsourced suppliers are also beginning to insist that their certificate be taken into account when preparing for and costing their annual SAS 70 audit, with consequently substantial reductions in both the cost of, and disruption caused by, the audit.

Are organizations beginning to recognize that, in fact, it *is* the badge on the wall that counts? Yes, as evidenced by the increasing number of badges. It took about seven years for the first 1,000 certificates to be achieved, but by April 2008 there are already over 4,500 successful certifications. And certification has a ripple effect: every organization that achieves ISO 27001 will expect its key suppliers to meet the standard. And this means that anyone who thinks the badge doesn't count will have nowhere to hide when the CEO comes asking why your competitors have stolen your lunch.



Richard E. Barry

IM Literature Review: Managing Electronic Records

Continued from last edition

Content

Evaluating the content of a book may be done in quite a few different ways. One such way is to ask and seek answers to leading questions. For example: how did it stack up with competition with similar titles; what did the authors (or editors) mean or promise to include; what are professionals in the field likely to want to see (although the most valuable literature often delivers important messages to the readers that they don't expect or want to see or know or care much about); and what would a reviewer want to have included in a book on this subject? I will comment on all the above aspects to one degree or another. I won't undertake the systematic comparative analysis that would be necessary to answer the first question. This is not a literature review, even on this particular title. Nonetheless, any reviewer's reactions to one book are bound to be influenced by others on the subject. I'm no exception, and that will come through intentionally or not.

How the book stacks up against the editors' vision for it may not be the most important approach, but it is probably the fairest. From a marketing point of view, taking the readership perspective may be the most important. The trick, of course, is for authors to sufficiently well understand the marketplace that their vision and delivery for the book captures and addresses market needs. I'll mention some topics that I consider important in managing electronic records, but those should be considered principally as provocations for discussion and for future writers rather than criticisms of this book. (If I were so smart, why didn't I write the book myself?) I therefore prefer to devote most time on the editors' and readers' perspectives.

What did the editors set out to do? In their own words, in the book's Preface, they took as for their challenge the proposition: "managing electronic records involves multiple roles, an extensive range of aspects covering the organizational, technical and legal issues, and ongoing exploration and investigation to achieve and share greater effectiveness and efficiency. To be successful, these all have to come together in holistic solutions, at the strategic and operational levels." In their wrap in the final chapter, they further elaborate these challenges:

- objects that are intangible in an environment that is virtual and dynamic;
- tools and solutions that are dynamic and constantly evolving; and
- tools that at best do not give priority to recordkeeping and at worst create havoc.

In the last chapter, the editors turn authors and provide an excellent cross-walk between the individual chapters using a strategic-tactical-operational construct. They also inform us on topics not easily considered in that construct: ethics and R&D and show how these elements are needed to complete the framework needed to play the long-game and win at it. Finally, they speak to futures.

The editors did broadly fulfill their promise as complex and multi-dimensional as the vision for the book was described. This was in no small way because of the tying up in the final chapter. At the same time, the chapters are so rich in content and so well written that the book would be a keeper simply as a collection of winning essays on electronic records.

What would likely readers expect? How do I know this? I don't, but I will postulate and hopefully stimulate further discussion by touching on two ways for thinking about this that may lead to conclusions about how readers will set their own expectations for this book: a) a sampling of other books with similar titles on the broad aspects of managing electronic records; and b) an indicative list of findings that recently have been identified and published in a U.S. federal interagency study on barriers to effective electronic records and the findings of a survey of U.S. and international users' attitudes about that study.

A few of the recent offerings on electronic record include: *Effective Approaches for Managing Electronic Records and Archives*, Bruce W. Dearstyne, Ed., 2002; *Managing Electronic Records*, 3rd Ed., by William Saffady, 2002; *Thirty Years of Electronic Records*, by Bruce I. Ambacher, 2003; *Records Management: Planning for the Electronic Records Archives Has Improved*, by Linda D. Koonz, 2004; and, 'fast-backwarding',

data breaches in this sector in the UK is probably much bigger than has actually been reported and at least as great as that in the public and regulated sectors.

The reported number of internally caused data breaches remains lower than external ones, but averages to around a third of those reported each year since 2000. Many data breaches are self-inflicted in that organisations adopt confidentiality regimes that make it difficult for people to actually do their job and, as a result, they bypass controls with unpredictable but inevitable data breach consequences.

The Ponemon report commented that "the investment required to prevent a data breach is dwarfed by the resulting costs of a breach" and "the return on investment (ROI) and justification for preventative measures is clear". Costs of data breaches legal costs, the costs of restitution, brand damage, lost customers and so on are significant; for financial services organisations, it was about £55 per compromised record.

Whilst not involving legal compliance, if an organisation has a credit card-related data breach and is found not in compliance with the Payment Card Industry Data Security Standard (PCI DSS), there are potentially severe contractual and financial penalties, including a bar on the business accepting payment cards.

All these factors make the protection of personal data and Data Protection Act compliance - a key business and compliance responsibility; the information security management standard ISO27001 provides a best-practice specification for an information security management system that would meet the requirements of the Data Protection Act 1998.



InoTec - AT YOUR SERVICE WORLD WIDE.

<p>Head Office InoTec GmbH Organisationsysteme InoTectalstr. 11 61509, Niederkrüchten GERMANY</p> <p>Tel: +49 (0) 6056 9708 0 Fax: +49 (0) 6056 9708 11 E-Mail: info@inoTec.de</p>	<p>Australia Asia InoTec Organisationsysteme Pty Ltd 87 Carole Street Fitzroy North, VIC 3068 Australia 0360</p> <p>Tel: +61 03987 4031 Fax: +61 03987 5101 E-Mail: inoTec@inoTec.com.au</p>
--	--

Act now to PREVENT DATA BREACHES



After twelve months of increasingly dramatic press headlines about failures to safeguard personal data records, it's time to assess the size of the issue and identify best practice steps for reducing the incidence of, and damage caused by, these data breaches.

The IT Governance Best Practice Report [Data Breaches: Trends, costs and best practices](#) identifies that spectacular data breaches, such as the UK's HMRC CD-Rom fiasco and the prolonged theft of TK Maxx credit card records, are not caused by the misdemeanour of a junior employee but arise, rather, from systemically inadequate information security arrangements at the organizations where the incident occurs.

A data breach is 'the unauthorised disclosure by an organization of personally identifiable information, where that disclosure compromises the security, confidentiality, or integrity of the data that has been disclosed.'

The Attrition database shows that the numbers of reported data breaches in the US increased from 22 in 2004 to 326 in 2006. The pattern in the UK and elsewhere is similar. Three developments in recent years make addressing this issue a real priority:

1. Identify theft is a low-risk, high return option for organized crime. Traditional crime, including violent robbery and theft, has clearly identifiable risks. It is easy to be recorded on video by CCTV, seen by witnesses or caught by means of DNA, and the returns are relatively low. High-tech crime, on the other hand, creates real problems for the police force and is, conversely, relatively low-risk for the criminal. Contributing factors include the perpetrator's anonymity, the speed at which crimes can be committed, the volatility or transience of evidence, the trans-

jurisdictional nature of cybercrime and the high costs of investigation.

2. Legal and regulatory compliance initiatives, such as the EU Data Protection directive and California's data breach disclosure law, SB1386, have both formalised the concept that personal data must be legally protected, and introduced penalties for failing to do so.
3. The proliferation of mobile data storage devices has changed the boundaries of where we store our data and effectively eliminated "fixed fortifications" as an effective tool for preventing data breaches.

The number of data breaches reported both within the US and the UK has been steadily increasing since 2006. In the US, the introduction of California's data breach disclosure law, SB1386, in July 2003 led to a greater awareness of data breaches and, as a consequence, greater reporting of them. Within the UK, the numbers of reported data breaches has also been steadily rising, with a large increase in the number of reported data breaches following the HMRC breach. The peaks in reported data breaches following the disclosure of the UK's HMRC data loss, suggests that there were and probably still are many data breaches that go unreported and research suggests that organizations are reluctant to officially report data breaches unless they have already been exposed. The evidence suggests that waiting to be found out is not the best strategy.

12% of reported breaches in the UK were at regulated financial services organisations. Those reported in the unregulated private sector are much lower. An extrapolation from this behaviour is that the likely scale and cost of

of the first international, interdisciplinary studies of this subject, produced by the UN Technical Panel on Electronic Records (1987-1989), which I had the honor of chairing and which gave me my own baptism of fire in electronic records. Anyone who has read one or more of these books may come to this one with the expectation of finding similar coverage. Hopefully they will also be looking for this book to fill in gaps in their earlier readings. I think they will discover that it does add some valuable new information, especially in the areas of human factors and organizational culture (Laeven, Fuzeau, Ellis); stakeholder building (An, Ellis); digital preservation (Marciano and Moore, Hofman, Ryan); standards (Hofman, Cumming, An); legal matters (Stephens, Ryan); R&D (An, Ryan); ethics and societal issues (Harris) and most especially post-implementation lessons learned from installed electronic records systems (Fuzeau, Ellis). Excellent overarching presentations that cover several of these topics are presented in McDonald's introductory chapter and Laeven's "Competencies" chapter. Of course, they were interwoven and related to one another by McLeod and Hare in the final chapter.

One example of an external view to consider what readers might consider important and thus might look for in a book on this subject may be found in a recent survey I conducted on barriers to effective electronic records that was produced by the Electronic Records Policy Working Group (ERPWG) an interagency group in the US government. Despite its orientation, its findings and recommendations were found to be highly relevant to survey respondents, including in other levels of government, in the private sector and academia as well as internationally. (See [survey results](#).) Among the topics that were high on the list of a high percentage of survey respondents internationally were:

- Records and information not managed as agency business assets;
- Records management not viewed as critical to agency mission or incorporated into automated business processes in a timely manner;
- Marginal support for records management has led to a lack of training, tools, and guidance for all staff;
- Poor integration of records management and IT disciplines;
- Need for greater and more effective leadership and clear records management guidance;
- Need to integrate recordkeeping into Enterprise Architecture;
- Standards to include recordkeeping compliance in audits and inspector general reports.

One might infer that these are not only seen as issues, but that readers would like to know more than they are barriers. Why are they barriers, and what can be done to overcome them? On most of these accounts, this book hits the mark with at least identification of the issue if not remedial suggestions. It is noteworthy that several of these concerns emerged as issues in the brilliantly done case studies, reinforcing their importance.

Architecture

In the area of architecture, more is needed in our professional literature. In the first chapter, McDonald speaks to "records architecture" independently but preferably as integral to a broader enterprise information management and IT architecture. I'm not so sure of the value of an independent records architecture, but certainly records management must be tightly integrated into the enterprise information and IT architecture to make for the implementation of a complete, effective and efficient electronic records system. Trying to deal with records

independently may operate in the other direction. In the last chapter, McLeod and Hare stress the importance of architecture and infrastructure at the tactical level. If those chapters constitute the bread in this meal, there is little on architecture in the sandwich between the slices. Exceptions to this appear, if obliquely, in Cumming's discussion of metadata and business processes and in Ryan's observation that the digital preservation function needs to be linked to the strategic business aims of the organization. Indeed it does, as do other key recordkeeping functions, not the least of which is electronic records capture. Architecture is about tightly knitting organizational assets, especially information and technology, to business processes most especially where business processes are automated. We need to generate literature that more rigorously addresses architecture on three kinds and levels: enterprise architecture, information architecture and technology architecture and how recordkeeping fits in. Leading recent books in the area of information architecture don't mention technology architecture and vice versa. Neither mentions recordkeeping as a service within the architectures. Yet all relate to an enterprise model or architecture.

Standards for Auditing and Compliance

The issue of standards for incorporating recordkeeping compliance into the audit process was considered crucial by 79% of the above-mentioned survey. Hofman devotes a welcomed section to this subject in his discussion of compliance, but much more is needed as increasingly tight laws and regulations that govern various business sectors (finance, pharmaceuticals, food, personal-health information, etc.) that may be national in their origin but are global in their impact since they apply to any organization wishing to do business in such countries. These events require recordkeeping to be seen in the context of special laws and regulations. Global companies failing to take account of such requirements in all countries where they wish to operate do so at considerable risk.

Implementation

There are few organizations that have implemented electronic records systems, and fewer references to them in books and even fewer appearances of the term "implementation" in indexes. This book stands out in this respect. With two outstanding chapters (10 (Fuzeau) and 11 (Ellis)) devoted to implementation case studies, two others, chapters (2 (Hofman) and 3 (Cumming)), with additional insights in major sections on implementation and another citation on the term in the index, there are some 29 pages citing the term at some level in the index.

In his review of Bruce Dearstyne's *Effective Approaches for Managing Electronic Records and Archives*, Matthew Veatch said, "[A]s authors in this excellent new collection of essays make clear, information professionals have developed over the past decade a variety of effective, context-sensitive electronic records management strategies." (See [TOC, book TOC, excerpt and review](#).) What we have not done so well with is implementing those strategies. Some of the finest writers about electronic records strategy are academics, especially those leading or teaching graduate ARM programs. While many universities have implemented or are in the process of implementing "institutional repository systems," using such systems as DSpace or Fedora to digitally manage faculty knowledgebases, these systems do not include the more rigorous functionality required for trustworthy electronic recordkeeping. Yet, few if any universities have actually implemented systems to manage their own university

records, except on a very limited basis in support of single business functions or processes. The fact that few university archivists are involved in teaching programs doesn't minimize that stark reality.

Despite almost universal implementations of e-government applications at all levels of government, government bodies are only slowly moving in the direction of actually implementing electronic records systems. There are case studies of implemented systems as part of the InterPARES project. Important as they are, most of these are special-purpose e-government, photo, GIS applications as distinct from enterprise ER systems. Local governments seem to be ahead of other levels of government. Several private-sector organizations have implemented electronic records systems, some using enterprise content management approaches. Many of them are unwilling to share this "competitive information," an interesting commentary on the implied importance of electronic records in the private sector. The bottom line is a dearth of completed implementations and related case studies from which to draw models and lessons learned to help stimulate additional implementations. Not surprisingly, a posting I made to several ARM professional discussion lists internationally in connection with this review created enormous interest. At time of this writing, within three days after my original posting, there were over 50 on- and off-list communications responding to this thread about the high level of importance practitioners place on obtaining more information on actual implementation assessments and the lessons discovered. This book makes a considerable, considerably important and timely contribution to the literature in this area that many professionals are obviously starving for.

Ethics (and Society)

Another salutary contribution of this book is its inclusion of ethics at the chapter level. As noted earlier, the 'long-game' vision the editors had included "vision and leadership, awareness and understanding, the environment and architecture, technical solutions, people issues and the things to be done." For the Harris chapter on ethics, I would submit "people and societal issues, as in fact the editors note as one of Harris' key messages. It is not only true in this case, but Harris' discussion is an important addition to a book that is not specifically on the subject of ethics and societal issues. Ethical and societal issues are subjects typically missing in ARM practice-oriented books, professional conferences and course outlines that aren't dedicated to ethics and society. Not everyone who goes for practice-based books on ARM in general or electronic records in particular is going to go for books focusing on ethics or society. Many may not readily see the relationship of ethics to ARM or electronic records. Moreover, ARM professionals tend to take the societal impact of what they do for granted or to be presumed as important and look at such issues and cases primarily from a personal perspective to the exclusion of broader societal perspectives. According to a "Report on the Society and Archives Survey" (by this author), most ARM professionals see a near total lack of understanding on the part of society of the importance of recordkeeping and the special demands of electronic records. Thus, where the subject is treated alongside other aspects of recordkeeping in more than a passing manner, as it certainly is by Harris in this book, it deserves to be noted.

As for topics I would be looking for in a book with this title, most of them are there, including the case studies, Hofman's presentation on standards and Marciano and Moore's on preservation. I've read some of the San Diego Supercomputer/NARA technical papers on very long-term,

persistent digital archives and was pleased to see how skillfully they crafted this presentation for a non-technical audience. A topic that I would have liked to have seen more coverage on, beyond the reference to PDF/A¹ in the excellent piece by Hofman, is long-term access and understandability of electronic records using "readers" that are designed to meet open standards (such as ISO-19005-PDF-A and OpenReader). I also share the views that I frequently hear from clients that much more is needed in the literature about ways for dealing with specific recordmaking technologies that are the bane of most ARM professionals. These include legacy "stovepipe" systems, email systems, enterprise resource planning (ERP) systems, and newer forms of business electronic records such as instant messages, Websites and blogs.

Bottom Line

Does *Managing Electronic Records* deliver what one might expect from the title? In the main it does, and better than others in many ways.

Context

The editors do an excellent job bringing out the relationship of chapters to one another and to their strategy-tactics-operations construct. They also make the chapter links to major cross-cutting electronic records issue areas such as standards, leadership, stakeholder building, and business systems analysis. I believe McDonald is the only other author who makes reference to other chapters in his presentation. ARM professionals should be good at context, beyond talking about metadata and archival description. One might hope for more contextual linking within chapters to others, but that may be asking too much in light of the difficulties of orchestrating the editing of a book like this.

The editors make another excellent contextual observation when they speak to the use of language in the book when, in the Preface, they talk about the differences in the use of such fundamental terms as "recordkeeping" and "records management." In Australia, the former term is the more inclusive and embraces the latter, which is seen not to include archives management. In the US and some other countries, it is the opposite. Perhaps it is because I feel that there is too much separation between archives and records management functions and professional organizations that is implied in the term "records management," I come down as the editors do with the Australian formulation and logic. Unfortunately, which is not mentioned in the book, the negotiating on the verbiage during drafting of ISO 15489 resulted in the adoption of "records management" as the all inclusive term, sadly in my opinion. The result was that "recordkeeping," as widely as the term is used internationally, appears nowhere in ISO 15489. This is not the venue for going into the reasons for this, but I hope as more countries gain more knowledge and experience with the Australian approach, ISO 15489 may be changed. Perhaps this observation by the editors in this book, though lightly treated, will help to draw attention to this matter as more than simply reviving the medieval debate on how many angels can dance on the point of a needle. It is really about how we (mis)communicate with one another in the most elemental of ways.

Structure (aka, user friendliness)

ARM professionals place more importance on document structure than most people. It is regarded as an essential feature of records. For some of the same reasons, and more, structure is



RECORDS AND INFORMATION MANAGEMENT AWARENESS FOUNDATION (rima foundation)

...promoting proper management and security of information



Presents:

Free Quarterly Training Programme



Covering:

Computer Literacy Session
Introduction to Computer (I)

Information Management & Security Session
Document Control & Management (I)
Managing Enterprise Records & Information (I)
Introduction to Information Security

For Whom

All federal and state parastatals, Local Government, Oil and Gas, Banks, Insurance, Maritime Industry, Construction, Engineering, Educational Institutions, Manufacturing, Telecoms, Law Enforcement, Legal, Health, Records & Information Management Professionals etc.

Date: Saturday, Dec., 13th 2008.
Time: 10am prompt
Venue: Ikeja Lagos.

Register online now at:
<http://www.rimaw.org/Registration.php>
Or Send your name, organisation, designation, telephone, email to
registration@rimaw.org

For support/sponsorship of the free quarterly training program please contact:

Ugochi - 08038392827
General enquiry - 8940451, 08023819008 or email: info@rimaw.org

BANDWIDTH DROUGHT?

Optimise your internet access with rock solid web caching and let your business grow

CACHEBOX web cache server appliances from Appliansys bring content closer to your users and deliver a number of real benefits to your business:

- Reduced internet bandwidth usage by serving content stored on the LAN
- Reduces bandwidth spend
- Faster performance on cached content
- Fewer user-perceived delays and increased user-satisfaction
- Less load on origin servers, saving hardware and support costs

For details of your local reseller please visit our website. Alternatively contact us at sales@appliansys.com quoting 'IM World Magazine 08'.



Save bandwidth now
WWW.APPLIANSYS.COM/SAVEBANDWIDTH

This is the age of silicon chips. So why is most of your company's information stored in a cardboard box?

No company should have to go to a warehouse to access vital information. Not when there's document management from Laserfiche®. Every memo, brief, plan and position paper in your company's history can be on your desktop in seconds, should you need it, with nothing more complicated than a simple keyword search. Isn't it wonderful what the 21st century has in store?

To learn more:

+233 21 247 334
+233 244 888 285
joseph@josanti.net

www.josanti.com



prohibit everything thus making mundane access tasks doubly difficult; some are lax and permit access by all to all, thus exposing themselves to a high degree of risk. Business efficiency relies on the right balance

Increasingly, organizations and their information systems and networks are faced with security threats from a wide range of sources, including computer-assisted fraud, espionage, sabotage, vandalism, fire or flood. Sources of damage such as computer viruses, computer hacking and denial of service attacks have become more common, more ambitious and increasingly sophisticated.

INFORMATION SECURITY CONCEPT

Confidentiality:

Ensure that information is accessible only to those who are authorized.

Provides assurance that only authorized users can read or use confidential or secret information.

Without confidentiality, anyone with network or Internet access can use readily available tools to eavesdrop on network traffic and intercept valuable proprietary information. For example, an Internet Protocol security service that ensures a message is disclosed only to intended recipients by encrypting the data.

Integrity:

Safeguard the accuracy and completeness of information. Integrity provides verification that the original contents of information have not been altered or corrupted. Without

integrity, someone might alter information or the information might become corrupted, but the alteration can go undetected.

For example, an Internet Protocol security property that protects data from unauthorized modification in transit, ensuring that the data received is exactly the same as the data sent.

Hash functions sign each packet with a cryptographic checksum, which the receiving computer checks before opening the packet. If the packet-and therefore signature-has changed, the packet is discarded. When used as "network integrity," it can be considered as the means of ensuring that the network is not permitting services or activities that are

DESKTOP SECURITY TOWARDS A SAFER COMPUTING

1. Keep your passwords strong, and keep them in your head.
2. Don't open it - you don't know where it's been...
3. Get anti-virus software. Use it. Keep it up to date.
4. If you can't trust the source you're downloading from, you can't trust the file.
5. Don't leave a computer you're logged into unattended or unprotected.
6. Data on paper is the same as data on the screen.
7. Your operating system needs to live and breathe. Don't let it get stale.
8. Don't use it? Lose it.
9. Watch out for those "Social Engineers".
10. Scanning is a two-way street.

against its policies. When used as "manual integrity" it can be considered that the information is not altered by someone else before being used.

Availability:

Ensure that only authorized users have access to all of the information and assets that they require. Assuring information and communications services will be ready for use when expected. It is the quality of information being at hand when needed.

Non-Repudiation

Rejecting or disowning or disclaiming as invalid; It provides assurance that a party in a communication cannot falsely deny that a part of the communication occurred. Without non-repudiation, someone can communicate and then later deny the communication or claim that the communication occurred at a different time.

The ability of the recipient to prove who sent a message based on the contents of the message. The quality can derive from the use of a Digital Signature on the message, which links the sender to the message.

A regular hand-written signature provides one form of non-repudiation. A digital signature provides another.

clusivity

Denying to a competitor any possible benefits he may derive from any information

a most important feature of professional and technical books. It may not be as important as their content, but it is in the sense that it is what makes their content usable and hopefully useful. This is because such books are not typically read in serial form from beginning to end, as most novels are. They may be scanned that way to give professionals a good idea of their scope and coverage, but mainly for future reference purposes. However, a principal use of such books is as reference resources. Someone wants to focus in a particular work, teaching or research situation on metadata, or preservation, or standards, or case examples of these things. They want to be able to pick up the books they know address their topic and find quite specific information in a timely manner without reading the whole thing from beginning to end again. The book's structure allows them to do that well or poorly. It provides what we might call navigation or finding aids and more generally its user friendliness. We know it when it is missing or poorly provided.

Elements of structure that authors may employ to help make their books as user friendly as possible include: table of contents, (high-level or detailed); chapter groupings under super-group headings or parts, an index, footnotes, a bibliography or reference list, and a study guide. A book may have many or all of these things and still not succeed in achieving, as a whole, a generally user friendly product, because it is possible and not uncommon for these things to be done poorly.

TOC, chapter groupings

Particularly because the mapping of chapters in this book is mainly addressed in the final chapter, it would have been helpful for the table of contents to attempt to group chapters according to their place in the strategic-tactical-operational framework with the R&D and Ethics chapters as peers to those framework sections. It wouldn't be perfect because of the cross-cutting nature of some of the chapters, but it might help the reader to make a decision to buy and read or not.

Index:

The index of a book that is going to be used for quick reference is a very important aspect of book structures its own right. It is even more important with an unstructured TOC such as this book has. This makes it a critical component of the book's success or lack thereof. Yet, index creation is often done by the publisher with little input from authors. When the index is not up to par, it is very evident to the reader. This book does about par with its index in very simple terms of the ratio of index pages to substantive pages expressed as a percentage. Using this measure, its index ratio is 7:193 or about 3.6%. This compares on par with Kahn and Blair's *Information Nation Warrior: Information Management Compliance (2005)*, 8:220 or 3.6%; and more favorably with Dearstynne's *Effective Approaches for Managing Electronic Records and Archives (2002)*, 2:160 or 1.3%. It compares less favorably with Cox and Wallace's *Archives and the Public Good (2002)*, 14: 317 or 4.4%. Contrasting from another field, Thomas Erl's *Service-Oriented-Architecture: Concepts, Technology, and Design (2005)*, has a ratio of 34:713 or 5%, and that book has a 16-page, four-tiered, highly structured TOC that makes it easy to find things. That book was written by one author, even with research inputs from others; but it is clear that the author devoted a considerable amount of time and thought to the TOC and index.

I observed numerous occasions where topics were covered in the text but not in the index. For example the term "architecture" appears once in the index but in at least five places in the text that I observed. Similarly, Harris speaks to many subjects other than

ethics, but suffers in the index with 20 references classified in two index terms: "ethics" and "South Africa." FOI is discussed in at least two chapters, but does not appear in the index. On the plus side, there is good cross referencing of some index terms, e.g., eight standards are listed by their number or short name (ISO 15489, DoD 5915.2, Dublin Core, CORBIT, etc.) but are also indexed according to the subject of the standard, e.g., records management, metadata, audit and certification.

Citations and Bibliographies

The editors and other authors provide a rich set of references cited in the chapter texts. The editors offer a very innovative approach in providing URL references in the book that I have not observed before. To save readers having to retype the Website addresses quoted in the text, [a complete list of URLs](#) is available on a companion website to the book.

The idea is exceptionally good and provides a considerable service for readers and an innovative integration of print and Web media. It will become an even greater and more useful innovation if the editors make arrangements to regularly test the URLs to ensure that the links remain hot and to update them when they change or disappear. It might be wise to place this page on a university or other Website. I do not have experience with Facet Publishing but, from experience with other publishers, I know that their own pages are subject to unannounced URL changes and page deletions.

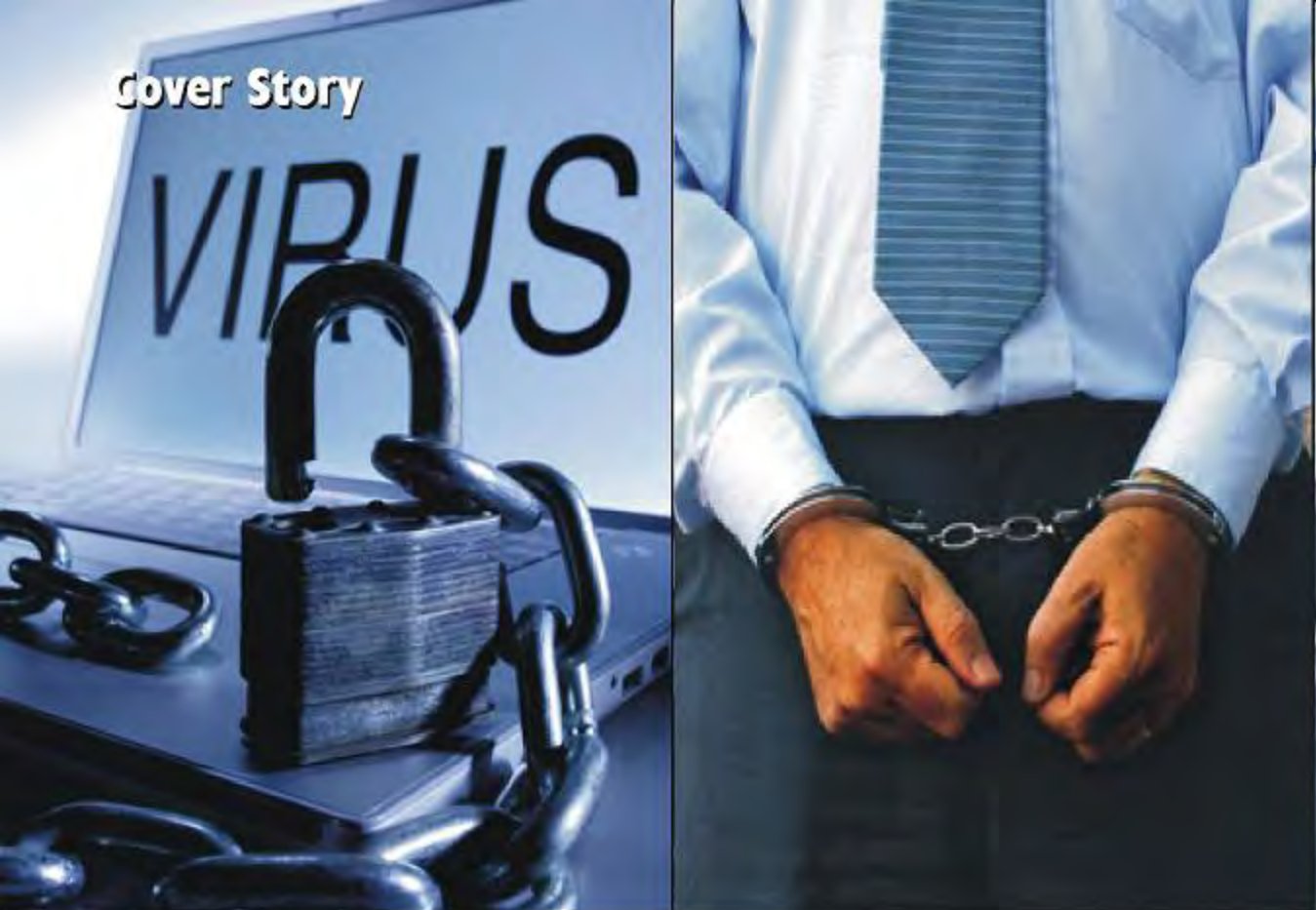
For the best reading experience, recognizing that many will not read this book in a single sitting I didn't say it was like a John Grisham or Alexander McCall Smith novel after all I recommend reading the Preface and Chapter 12 first, followed by McDonald and Laeven before proceeding to the other chapters. This isn't a comment on the best chapters. If it were, Chapters 10 and 11 and others would be high on the list. Rather it is my opinion on the best sequence of chapter reading. Chapter 12 is logically and very appropriately placed where it is in the book as an excellent wrap, much as might be done if these were papers presented at a conference. However, especially for the uninitiated, it will ease the reading experience of other chapters if Chapter 12 is read early on.

While there is much gnashing of teeth about the low priority, low resourcing and low status of the ARM functions in organizations, there is little ownership of why that is so. Much of it is due to the fact that professionals in the ARM field have been singularly unsuccessful in communicating adequately to their own executives about what they do and its importance. Too much is said about "the mandate" for ARM and too little about the business case for it. This book offers some excellent communications that could be effectively used as a short-term way of addressing that problem. My guess is that if executives read even the Preface and Chapter 12, they would soon find themselves doing some non-linear dipping into the other chapters. They might even steal themselves ultimately to read the whole book given that one of its other attractions is that it comes in under 200 pages quite an achievement in itself for the level and quality of content it contains.

SOURCE FROM

Rick Barry

Is an internationally known management consultant and cofounder of the Open Reader Consortium who lives with his wife, Linda Cox, in the Washington D.C. suburb of Arlington, Virginia. He is Principal of Barry Associates where he brings to bear interdisciplinary skills in information management.



Online Banking in Nigeria: PROTECTING ONLINE TRANSACTIONS IN BANKS

By DAVID ISIAVWE
(CISSP, CISM, CISA, CGEIT, SBCL, FCA)
GM & HEAD, GROUP INTERNAL AUDIT (UBA PLC Nigeria)

The world has reduced to a global village through the use of Internet. Hence, distance is no longer a barrier for trade. A buyer, from the comfort of his office or home can order and pay for goods without knowing or having any physical contact with the vendor. This is made not only possible but convenient through the advent of e-commerce.

The Nigerian economy has witnessed improvements over the past years, moving from its rudimentary level during the early years of trading to the current state of sophistication comparable to other economies at the same level of development.

However, the efficiency of the system is hampered by the unusually large cash usage as a mode of effective payments.

TRADITIONAL BANKING

- Traditional Banking entails that you have to be physically present in the bank to consummate transactions.
- Payment in bank branches and confirmation of payments are usually lengthy and laborious.

hardware, software, personnel policies, information practice policies, disaster preparedness, and the oversight of all these areas.

Absolute security is impossible to achieve in practice and the quality of a given security system is relative. Within a state-model security system, security is a specific "state" to be preserved under various operations

Information Security is no longer just an issue for I.T managers - a single breach of information security could cost an organization hits hard earned profits whilst doing irreparable damage to its public image and reputation. Based on risk assessment, we are usually in a position to measure the consequences of information theft.

An organizations capacity to trade profitably will depend on its ability to manage this risk effectively.

Factors affecting the level of information security in an organization

- The value of the organization data.
- The volume of the organization's data.
- The security that customers, partners, and suppliers expect from the organization.
- Legal obligations.
- Existing security.
- The sensitivity of the information.
- The criticality of the information.
- Protection of information from accidental or intentional misuse by persons inside or outside of an organization.

Purpose of Security

The purpose of security is to protect both the system and the information it contains from unauthorized access, misuse within and outside. Information Security is achieved by implementing a suitable set of controls, which could be policies, practices, procedures, organizational structures and software functions.

These controls need to be established to ensure that the specific security objectives of

the organization are met. Information Security management ensures business continuity and reduces business damages by preventing and minimizing the impact of security incidents. Research has shown that fraud or cases of IT abuse often occur due to the absence of basic controls, with a significant amount of all detected frauds found by accident

All information in all departments is at risk from a number of threats. While equipment theft is a real problem, the most damaging aspect is the loss of data and software.

The Internet exposes organizations to an increased risk that networks will be accessed improperly, data corrupted and viruses introduced.

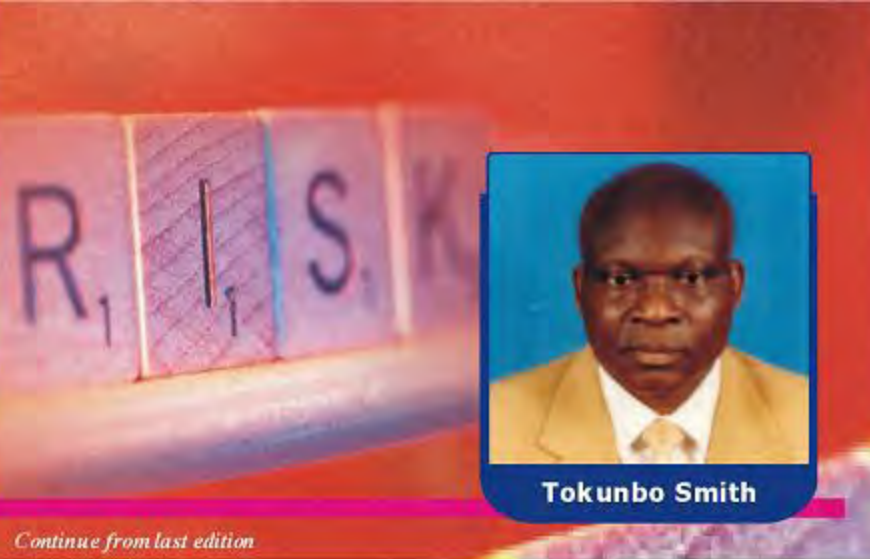
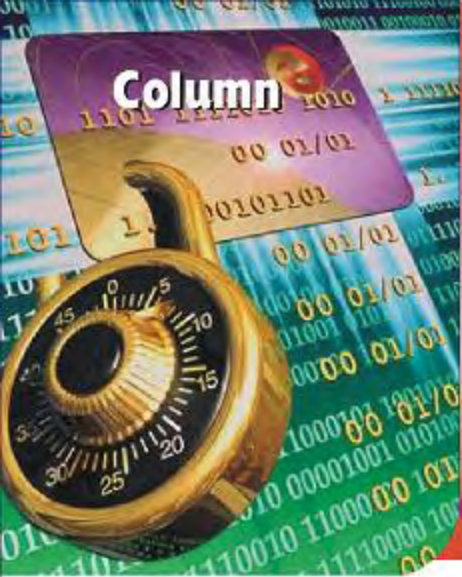
The percentage of organizations reporting hacking incidents has increased, with telephone systems also a target. Not all breaches are the result of crime. Inadvertent misuse and human error play their part.

Virus infections are still the single most prevalent form of abuse. More commonplace and just as destructive as crime, are threats like fire, system crashes, and power cuts. Poor supervision of staff and lack of proper authorization procedures are frequently mentioned as the main causes of security incidents. Companies vary in their approach to preventing security breaches - some

7 COMPUTER SECURITY TIPS FOR STUDENTS

These tips can help protect the computers you use in school from viruses, hackers, spyware, and other attacks.

1. Perform basic computer safety maintenance (Use an Internet firewall, Update your computer, Use up-to-date antivirus software, Use up-to-date antispyware software)
2. Don't open files from strangers
3. Help fight spam and online scams
4. Learn how to protect yourself from spyware
5. Take precautions when you go wireless
6. Password protect your computer—and lock it
7. Back up your work



Tokunbo Smith

Continue from last edition

Information Security Fundamentals

SECURITY

As economies of countries regress unemployment/under employment rates increase, so also criminal activities keep increasing on a daily basis. Even in countries with fairly stabilized economies, issues of people born with criminal tendencies cannot be overruled.

The essence of security therefore is to create difficulty for the thief and make him work harder. Criminals do not want to be caught in the act, they want to enjoy the fruit of their "labour", so the harder the target, the more discouraged they become.

The security of a system can be protection against unwanted event such as the invasion of privacy, theft, and the corruption of information or physical damage. Security in a nutshell is the protection of life and property, prevention of loss and waste, prevention and detection of crime, for the purpose of continuity. In summary, security is SAFETY!

Security of a system is a function of the state of being free from

danger or injury: freedom from anxiety or fear; Protection of information systems against unauthorized to or modification of information whether in storage, processing or

IS YOUR COMPANY KEEPING INFORMATION SECURE?

Are you taking steps to protect personal information? Safeguarding sensitive data in your files and on your computers is just plain good business. After all, if that information falls into the wrong hands, it can lead to fraud or identity theft. A sound data security plan is built on five key principles:

1. Take stock - know what personal information you have in your files and on your computers.
2. Scale down - Keep only what you need for your business
3. Lock it - Protect the information in your care
4. Pitch it - Properly dispose of what you no longer need
5. Plan ahead - Create a plan to respond to security incidents

in transit, and against denial of service to authorized users, including those measures necessary to detect, document and counter such threats.

Although information security is by no means strictly a technical problem, its technical aspects (firewalls, encryption password and the likes) are important.

Information security is an increasingly high-profile problem, as hackers take advantage of the fact that organizations are opening parts of their systems to employees, customers and other businesses via the Internet

Information security protects information from a wide range of threats in order to ensure business continuity, minimize business damages and maximize returns on investments and business opportunities

Security encompasses all of the safeguards in an information system, including

- The use of cheques, not readily acceptable as there is the usual suspicion that it will "bounce".
- The clearing period is longer depending on the location.
- Improper means of identification

What are E Channels?

E Channels in Banking are the channels through which customers are served other than through the traditional bank branches which include the use of:

- Automated Teller Machine (ATM)
 - Debit Cards
 - Credit Cards
 - Point of Sale Terminal (POS)
 - Paydirect
 - Kiosks
 - Webpay
 - Internet Banking
 - Telephone/Mobile Banking
 - SMS Banking

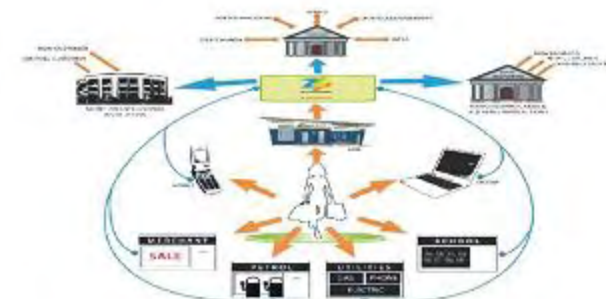
Before Online banking

- Long queues in banking halls
- No banking services after close of business
- Physical presence required for all banking transactions
- High security risk associated with cash handling
- Absence of self service banking
- Cumbersome process of transferring funds
- High cost of cash management
- Heavy reliance on the use of cheques /draft
- Long turnaround time for processing transactions

Why Banks are using online Banking today

- To displace cash/cheque payments
- To protect and grow customer base
- To deepen customer relationships and increase loyalty
- To provide a defense mechanism against competition

- To reduce queues in our branches
- To increase profitability (long run)



How Good is your backend

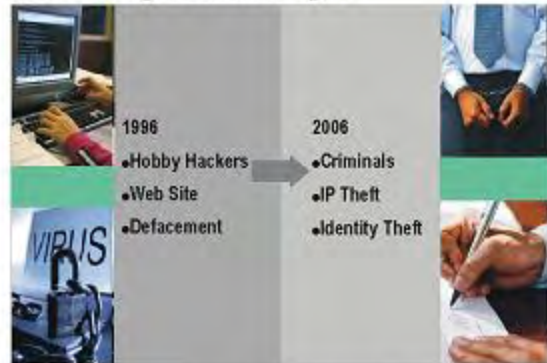
- Internet banking relies on your back end infrastructure
 - How good are your communication links?
 - Is your website up?
 - Can it connect to your Internal database?
 - Is it secure?
 - How much functionality do you provide?
- Data Security - "If companies want to prevent data breaches, damage to their brand, and huge fines, they must ensure data is protected both internally and externally, and make sure they constantly track new data privacy regulations."

Security is Now a Business Issue

- No longer just a technology issue
- Security breaches impact business bottom line
 - Online Banking Services provides ease of access to customers and unlocks business potential, but ...
 - Also invites higher business risk
- Complexity and severity of security threats have increased dramatically
- Governance and Privacy regulations emphasize strict security controls



Information Security in Banking Has Changed



Ramifications of Security Breach

- LOST ASSETS**
~21% of enterprises are worried about a decline in stock price
- LOST REPUTATION MARKET RISK**
- LOST CUSTOMER LOYALTY**
- LOST REVENUE**
- REGULATOR INTERVENTION**

The Information Security Layers



Challenge: Enforce Access Control

- Fragmented security policies
- Too many user id's and passwords
- Orphaned accounts
- Expired access rights
- Lack of aggregated audit and accountability
- Stolen passwords
- Manual provisioning requests prone to errors
- Network administrators unaware of organizational and role changes



Securing Access to Banking Systems

- Centralized security and policy management
 - Consistent policies enforced across the Institution
 - Enterprise wide visibility of users, access rights, audit data
- Automated provisioning / de-provisioning
 - Role based user provisioning and de-provisioning
 - Automated updates triggered by user status change
- Federated access across enterprises
 - Secure, affordable identity integration with partners



OTHER CONTROLS

The following techniques are also necessary to combat Online Banking Frauds:

- Encryption - Private and Public-key cryptography
- Masking of Password
- Pin Protection
- Implementation of DMZ
- Intrusion Detection System (IDS)
- Firewalls

Government departments, financial institutions and manufacturing companies all made use of microfilm with active folders held in paper format and closed files held on microfilm jackets or roll microfilm. Several suppliers also developed computer output microfilm (COM) recorders which allowed computer data to be recorded directly onto microfilm at very high speed. The use of microfilm peaked in the 1980s and billions of documents were recorded onto this medium.

Microfilm made a secure archive format and huge collections remain on microfilm today. However, it was never a very easy format to use and was not practical for the management of active documents. It survives today as an archive medium but on a relative small scale.

Computers in the office

In the 1980s the entry level of cost for computing came down considerably, and alongside shared mainframe, and minicomputers we saw the introduction of personal computers in the office. Word processing became widespread with staff creating their own documents in electronic format. This was followed by spread sheets and many other personal productivity applications.

To start with, these office computers were seen as a way of making us more productive at producing paper documents, so paper remained the format of choice for holding master documents and records. As Microsoft achieved dominance in the personal computer world with its Windows operating software and Office applications to a level de facto, standardization was achieved and demand grew from users who wanted to manage their electronic

documents online. Users started to develop ad hoc hybrid records management solutions were internally generated electronic documents were held in electronic folders on shared or personal drives while incoming documents were held in paper folders in shared locations. The forward looking used the same set of metadata to index the paper and electronic folders so all the information held on a particular client or topic could readily be retrieved. So, as well as hybrid paper and microfilm records systems, we now have hybrid paper and electronic records.

Tools for managing structured data were developing throughout this period and by 1990s they include relational database management systems, simple flat-file database and data spreadsheets. The choices related to the volume of data to be managed, the value of the data, the potential number of users of the data and the type of processes that need to be carried out. Individuals and teams were starting to use spreadsheets and PC database. Team and departments were managing databases and specialized applications built on top of relational databases. Government departments and large commercial organizations started to use computer systems to manage paper records. A computer database was used to hold the metadata needed to uniquely identify each folder and folder parts, to track the location of folders as being in the registry or out on loan to users, and the status of folders as open and closed. Some of the suppliers of such records management or registry software have gone on to develop electronic record management and ECM solutions.

SOURCE FROM AIIM

A Brief History of ENTERPRISE CONTENT MANAGEMENT

The all-paper environment

One hundred years ago, all the information which an organization held, the corporate memory would have been held on paper or in the brains of the employees. Data was recorded in tables, in ledger books and documents comprised handwritten text on a range of sizes of paper. When mainframe computers were first introduced after the Second World War, some of the ledgers were replaced by temporary digital storage, but for safekeeping most computer data was also out put paper in the form of bulky computer printouts.

Paper and microfilm

A photographic medium called microfilm had been in existence for many years in niche markets such as banks, where cheques were regularly microfilmed. In the 1970's alongside the rise of the computer, the use of microfilm



Microfilm made a secure archive format and huge collections remain on microfilm today. However, it was never a very easy format to use and was not practical for the management of active documents.

increased as a way of reducing the space occupied by inactive and archival paper records. Paper folders were used while documents were active but when they became less active, the paper was microfilmed and held in a range of microfilm formats to save space and preserve them. Large volumes of valuable reference documents were also microfilmed and duplicates were made and sold as a low-cost form of publishing. There were roll microfilm formats including 16mm and 35mm and there were also what were described as flat or unitized formats including microfiche, microfilm jackets and aperture cards.

Security & Identity Management Traditional Approach to Access Control in most Banks



What Must Be Done by Banks?

- Technical: Institutions must understand the issues, stay current and invest in research
- Setup Forensic and Investigations unit
- Human Capital: Expose staff (especially ICT team) to global trends and new knowledge
- Legal: ICT Policy is key, and banks must support national legislation against cyber crime
- Socio-Economic: Get potential criminals out of your way by reporting fraudulent cases to ICPC, EFCC, SSS and POLICE

- by banks to capture collections. It can only be accessed by combination of user id, password and PIN.
- It was possible to process Bank A's transaction from Bank B's network. Unknown to banks?
- Interswitch can identify and trace all transactions to banks through their dedicated proxy server IP address
- POS were configured by tripartite of Banks, Service Providers and Interswitch. Record management?

CASE STUDY

- Bank A teller discovered about N2.7m on her till balance at the end of day on Friday.
- The teller and the whole branch could not trace the source of the transactions before they went home.
- By Monday morning, the teller's till balance had increased astronomically to about N75m.
- The transaction journal generated on Monday revealed that the branch teller's till was debited through Pay direct while several debit cards from many banks were credited.
- Electronic transfers were effected into many cashcards (i.e. about 150 cards) through POS
- Within the 72hours,
 - Cash were withdrawn from ATMs;
 - Purchases were made from several merchants' POSs
- Bank A reported the case to the Interswitch and Police.
- The outstanding balances on the cashcards were quickly blocked by the affected banks.
- Police commenced their investigations arresting key staff from banks.

Control Measures

- PayDirect transactions must be tied with Teller's till balance
- Collections through PayDirect must be remitted quickly
- Inability to log on from another bank's PayDirect website
- Tellers must not compromise their user id, password & PIN
- Elimination of Deposit/Transfer functionality on POS
- Reduction of Transaction Limits
- Efficient Investigation & Reconciliation team to review reports
- Controlled User Security Management
- 24/7 Call Centers to block/hotlist cards
- Default pin must be activated on card before cash loading
- Installation of Camera on ATMs
- Blocking of Phishing websites
- Good Record Management
- Strong awareness campaign on associated risks relating to PIN compromise - adverts in newspaper and pasting of posters in branches.

Learning Points:

- The fraudster got a Bank A's teller user id, password and PIN to log into Paydirect Application of Bank A. How?
- Paydirect Application is a web application used

EDUCATION!!!

- PIN & Card Protection campaign
- Report of Stolen Phones, wallets, etc
- Fake Text Messages
- SCAM emails

Thinking of
Digitization & Data Extraction
From Huge Volumes of
Multi Sized Documents...



...We Have Just the Right Combination for YOU






Rs. 12,990/-
 Rs. 3,599/-
 Rs. 7,199/-
 Rs. 5,99,999
 Rs. 2,12,000

20% DISCOUNT

NETSPIDER INFOTECH INDIA LTD.
Mumbai office
 B-104, Rebelo Enclave, Subash Nagar, 23rd Cross Road, MDC, Andheri (east),
 Mumbai 400 093, Maharashtra, India
 Tel: +91 -22- 40058043 HP: +91 98208 00633 E mail: sales@nii.in Web: www.nii.in
Delhi office
 Tel: +91 -11- 26485139 HP: +91 99990 61589 E mail: delhi@nii.in
UP
 HP: +91 9918517272 **Channel Partners Invited**

Net Spider
www.netspiderindia.com

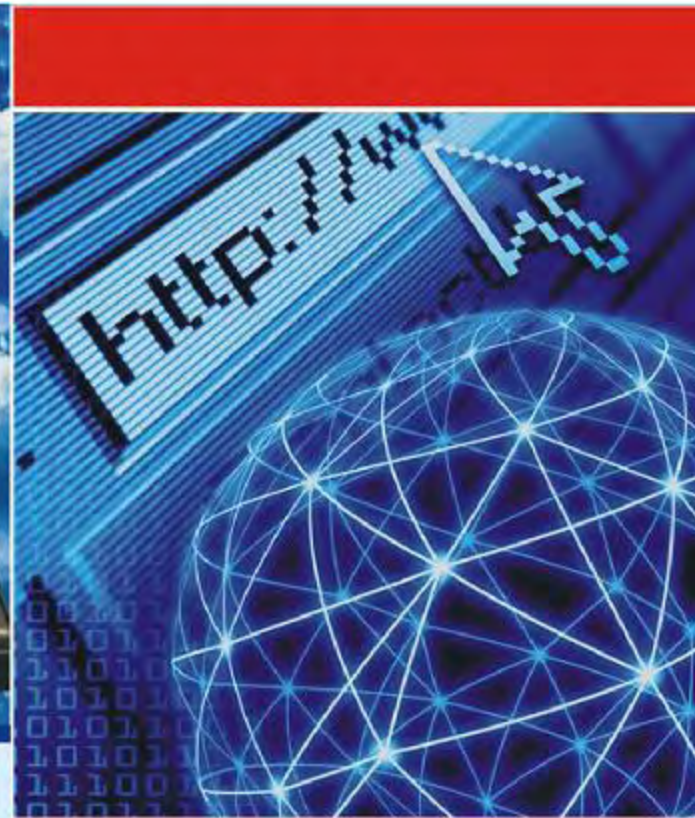
Document Imaging & Management Solutions Company
 |Distribution |Technology| Processes | Consulting |

Buy online at <http://www.surehorizons.com>

Business Management Made Easy !!!



- ☀ Over 25,000 downloads.
- ☀ Satisfied customers in over 15 countries.
- ☀ 40+ downloads site awards.
- ☀ Covers over 20 key business functions.



LAPTOP
Galleria

Suite 30
 30/ 31 Otigba Street, Computer Village Ikeja, Lagos.
 7754587,8931170,4976747, 08033047522

Solcara
 Connecting people to
 Information that matters



Cross Section of Attendees



Attendees Networking



Cross Section of Guests and Attendees



Registration of Participants



President RIMA Foundation



Exhibitor @ RIMAW 2008



Mr. Sorunke Laja answering questions from Mr. Olugboyege and Mr. David



Mr. Jide Awe



Mr. Smith Tokunbo left, chatting with Dr. Jide Ayenidi



Ushers at the registration desk



RIMAW 2008 Exhibitors- Blue and Check Technologies Ltd, Digital Persona, Upperlink Ltd. & GTBank



From left Mr. Oyedokun, Mr. Smith Tokunbo and Dr. Jide Awe



Union Bank Rep. with the President, RIMA Foundation



Registration desk



RIMAW 2008 Exhibitors- Microworld, Solcara Inc Wolexdok Micro-process or, McAfee.



From left Mr. Jide Awe and President RIMA Foundation Mr. Oyedokun



Segun Akano MD/CEO, Upperlink Limited



Mr. Sorunke Laja and Mr. Oyedokun



Mr. Smith Tokunbo



Dr. Jide Ayeni-DG CIREM



Mr. Sorunke Laja (UBA)



RIMAW 2008 Organising Committee



The president in the Middle with ushers during the events



Selected guests & RIMAW 2008 Organising Committee



RIMAW 2008 Attendees



RIMAW 2008 Attendees



Mr. Jide Awe (JIDAW.COM)



Welcoming guests to the Awards venue



Cross section of guests



Members of the high table



Guests



Hon. Tijani Ojo



Guests during the Awards night



A guest stepping into the venue



Dr. Martin Ikpehia Launching IM World Magazine during RIMA Awards Night



Oyedokun Ayodeji O. President of RIMA Foundation during the welcome address



President of RIMA Foundation with Guests



Press & guests



Mr. Ajao David & Union Bank Representative



Entertainers during the event



Xerox - RIMA Award Recipient



SEC - RIMA Award Recipient



President of RIMA Foundation with Guests



BTV representative giving a vote of thanks to the organisers of the Awards



President, RIMA Foundation during a press interview



Zenith Bank - RIMA Award Recipient



Opentext - RIMA Award Recipient



Zinox - RIMA Award Recipient



Spatial Tech. - RIMA Award Recipient



Buffet stand



BTV - RIMA Award Recipient



SEC - RIMA Award Recipient



IGI - RIMA Award Recipient



DigitalPersona - RIMA Award Recipient



Buffet time



Guests



Buffet time during the Award night



Guests



Members of the high table

"The significant problems that we face cannot be solved at the same level of thinking we were at when we created them." Albert Einstein

QUESTION OF THE MONTH

Question: How do I determine if my records management/filing system is effective?

By: Oladele Johnson CNL Lagos

Answer: You would be required to make a study of your system. Conducting such a study is no more than taking an inventory of the records in your files/system.

Some of the basic questions you should consider asking are:

- What are records?
- Where should they be filed/stored?
- Who uses the records?
- How often are they used/accessed?
- How are they used/accessed?
- How are the records referred to?
- What is the size of each record?
- How many of each record are filed?
- Who else has copies of the same record?

or legal requirements

- You are using your filing system or equipment for non-records storage.
- Your file folders are too full for easy access.
- Your filing drawers or shelves are too full for easy access.
- You are not finding the information you require in the first place you look.

With all your findings above, your analysis is complete, your records inventory reveals the strengths and weaknesses of your records management/filing system.

Once you have analysed your records inventory, you should determine:

- Best arrangement of the records.
- Type of media to be filed (paper, micro film, se pia, tape etc).
- Proper equipment for adequate storage and retrieval.
- Proper systems to complement the equipment.
- The required record retention schedule and facility.

Also check if your filing system shows any of the following symptoms:

- You can not find the information you need, it is difficult to obtain due to your system or lack of one.
- You are repeatedly having to expand your file system capacity.
- You are maintaining duplicate files of the same information.
- You are filing material to protect the function and not because of information.

Post any information/content/record/document/security questions for an expert to resolve for you and your organisation Send email to: info@rimaw.org



RECORDS AND INFORMATION MANAGEMENT AWARENESS FOUNDATION (RIMA FOUNDATION)

...promoting proper management and security of records & information

Presents



Electronic Records Management Certificate Programme (Practitioner, Specialist and Master)



ready. aiim. learn.

The ERM Certificate Programme explores records management in relation to business needs in both public and private sector, embracing all records, but with a particular emphasis on electronic records.

The ERM Certificate program consist of three levels: Practitioner, Specialist and Master.

Two-Day ERM Practitioner and Specialist

Achieve the practitioner and specialist qualifications by attending the first 2-day or last 2-day respectively.

Four-Day ERM Master Training Class - call for dates

The ERM Master Certificate Program covers the full content of the ERM Practitioner and ERM Specialist programs in addition to a case study exercise. The class provides complete coverage of records management in the electronic environment for people working in both the public and private sector.

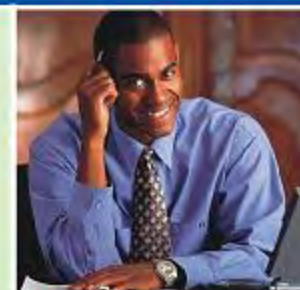
Date: 24th-27th March, 2009 & 24th-27th August, 2009
Venue: PROTEA HOTEL 1, Mogambo Close, Maryland Estate, Ikeja, Lagos State, Nigeria, West Africa.



Head Facilitator: Hanns Köhler-Krüner

Director Global Education Services (EMEA)
Association for Information and Image Management (AIIM) - UK

For Registration and Further Details log on to
http://www.rimaw.org/Registration.php
E-mail: info@rimaw.org, registration@rimaw.org
Telephone enquiry: 01-8940451, 08023819008



- Learn global best practices for planning and implementing ERM
- Discover real world solutions and best practices for the challenges you face
- Learn from experts in the field who are able to answer your questions, address your comment, and accept your feedback
- Position yourself to be tomorrow's leader by enhancing your business and professional skills

