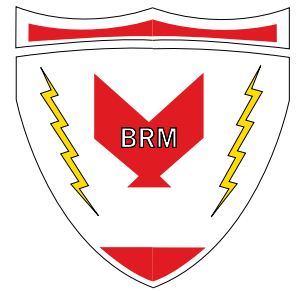




The
BUSINESS RECORDS MANAGEMENT
BULLETIN



A Service of **BUSINESS RECORDS MANAGEMENT**

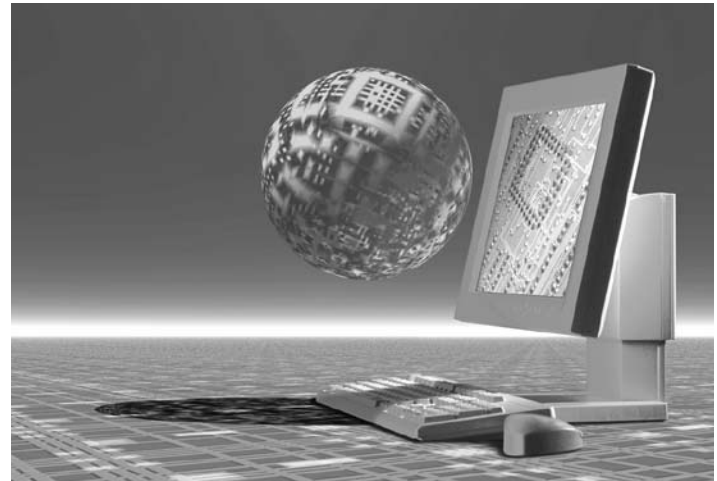
1st Quarter 2007

INTERNET SECURITY – HOW FAR HAVE WE COME?

In the beginning, the Internet was nothing more than a cold war response to Sputnik. A series of radar stations were linked together in a network in order to communicate information to each other. From this modest start, university computer labs combined resources to introduce the concept of timesharing nearly three decades later. By the early 1980s there was regular communication and electronic mail across networks like ARPANET, BITNET, TelNet, UseNet and NSF-Net whose launch in 1983 is generally thought of as the point of origin of the modern Internet. The Internet was, and remains, a networked array of computers linked together by cables. What we think of as the modern Internet, actually called the World Wide Web, did not come into being as a concept until 1991. The first web pages created in Hypertext Transfer Protocol (HTTP) did not appear until 1993. For a very interesting look at historical web pages visit “The Wayback Machine” found at www.archive.org/index.php. The site contains snapshots of more than 85 billion web pages from 1996 to the present.

REVIEW OF COMMON THREATS

The first recorded computer virus outside a lab occurred in 1982 on a computer running Apple DOS 3.3. The first PC virus was recorded 4 years later and originated in Pakistan. Prior to large-scale Internet connectivity viruses were most frequently transmitted by contaminated floppy disks used to transfer programs and data between computers. Transmission via the Internet began to occur in the late 1980s on BBS (bulletin board) or newsgroup systems such as USENet. Trojan horse virus infections were most often spread through the sharing of pirated software programs or shareware.



In the mid-1990s macro viruses made their debut. This type of virus exploits vulnerabilities contained within legitimate programs such as Microsoft Word™ or Microsoft Excel™ programs; these programs are capable of memorizing a series of keystrokes or commands in order to more quickly complete repetitive tasks – these are called macros. Because Apple™ computers also utilized these programs, viruses were also written to infect the Mac OS. Macro viruses are difficult to detect due to the fact that macros are a legitimate function of the software. These programs now allow macros to be detected, if they are present, and disabled prior to opening the file. One famous macro virus was the “Melissa” virus.

While viruses of all types seek to do harm to individual computers, computer worms seek to harm computer networks. Worms were invented in a laboratory setting in 1978 but the first widespread network attack of a computer work occurred in 1987. This attack completely disabled IBM’s international network and BITNET. Worms may be used to create alternate points of access to the network which enables the sender to effectively take control of a network in order to send spam, e-mails or for other purposes. Computer worms such as ILOVEYOU, Sobig and Mydoom created zombie networks for spammers.

A computer fraud technique known as phishing has become a significant modern threat. Phishing is an attempt to force a user to reveal personal information by responding to what is seen as a legitimate request. Users may receive an e-mail or instant message from a financial institution, E-bay account or other legitimate entity requesting that the individual respond by verifying billing information, account information or identity by clicking a web link. If the criminal is successful, sensitive personal information, including credit card information, may be obtained under fraudulent circumstances and used without the permission of the owner.

This practice originated on AOL in the mid-1990s. In June 2005 more than 15,000 phishing attacks were reported.

A variation of phishing is called spoofing. This technique is employed by computer worms such as ILOVEYOU to change e-mail header information in order to make the e-mail appear as though it came from another person. This is accomplished when the worm searches the e-mail address book of the infected user and begins to send infected e-mails from persons in the address book to other persons contained in the address book. Very often the individual who is the supposed "sender" of the e-mail has no idea that e-mails are being sent with their name identified as the source of the mail.

Denial of service attacks are another relatively recent development. In this type of attack a network is flooded with e-mail or requests for service in order to exhaust the resources of the network. Another type of denial of service in some systems is using an incorrect password with a legitimate user ID in order to lock the account of the legitimate user. These types of attacks may be initiated by disgruntled current or former employees, irritated customers, or by random spammers as a means of retribution against the organization.

STRATEGIES FOR DIGITAL INFORMATION PROTECTION

The list of potential causes of injury to digital information assets is almost limitless. Network users must be constantly on guard for suspicious e-mail traffic and must closely adhere to security practices and procedures outlined by IT professionals who administer the network. An individual failure could expose the complete

network infrastructure of the company to costly delays and downtime, information destruction or misuse, and could prove damaging to the reputation and brand of the organization. There are three critical areas of focus for network security: prevention, detection and response.

According to Computerworld Magazine and Trusted Strategies LLC, 84 percent of serious network attacks could have been prevented if organizations would have taken steps to verify the identity of computers connecting to their network, in addition to requiring user names and passwords. (This statistic considers all network attacks in which federal officials were able to charge someone with a crime.) This indicates the importance of protecting user names and passwords from theft or misappropriation. **Change user names and passwords frequently and guard them against theft or misuse. IMMEDIATELY DELETE PASSWORD ACCESS OF ANY TERMINATED EMPLOYEE.**

Social networking (Instant Messenger, etc.) has become much more common in the workplace and is a frequently used channel to deliver malicious code. If company policies permit the use of social networking for business purposes, extreme caution should be used when interacting with unknown persons.

Create policies that eliminate or greatly restrict social networking. Train employees as to the dangers of virus delivery through messaging, web advertising and media software.

One of the most important preparedness actions that can be taken is to ensure that a complete backup of all digital data is kept offsite and out of the control of any employee. This is **absolutely essential** in order to prevent acts of employee sabotage. Restoration from backup media should be periodically tested in order to ensure that backup media is functioning correctly and that systems can be restored in the event of a major attack or other disruption. **Store a complete set of backup media offsite and out of the control of any employee. Periodically test the restoration capabilities of the backup.**

Intrusion detection systems may be installed at the network, application or host level and use sensors and other techniques to monitor and log traffic. Some systems also look for anomalies in the system in order to

alert IT personnel to the possibility that an intrusion is taking place. Devices such as network, server and application firewalls help to restrict access and limit the possible points of intrusion. An additional technique called “honeypots” places decoy network resources within easy reach of intruders. This functions similarly to a “canary in a coal mine” to provide early warning of danger.

Ensure that robust firewalls and intrusion detection systems are installed, properly functioning and closely monitored.

Microsoft’s best practices document on network attacks suggests the following strategies during and after a network attack:

- Identify the nature of the attack – an effective response strategy is difficult until the type of attack is known.
- Find the source and shut it down – This could involve pulling infected computers off the network, close ports, block the attacker’s IP address or coordinate with your ISP if the source is beyond your immediate control.
- Protect evidence – logs and other information can be vitally important to law enforcement as they investigate the incident. Make sure to preserve all information related to the attack.
- Locate all affected machines – Run appropriate antivirus or patches to repair machines that are involved in the incident.
- Don’t reinvent trouble – When reinstalling operating systems and files, use a backup that you know has not been compromised. Don’t try to patch your way back to functionality; the risks are too great.

Network security is the responsibility of every employee who has access to the network. Vigilance, attention to detail, good training and adherence to procedures are key to helping protect your digital information. Preparedness by continuous rotation of data backups offsite provides an effective route for restoration in case of attack. Ask your offsite data protection partner for more information.

Records Management Added to List of Clinger-Cohen Core Competencies



IT managers need to know more about records management. That’s the message they received when records management was added to the Clinger-Cohen Core Competencies latest version. The CIO Council, which serves as the principal inter-agency forum for improving the federal government agency information resources, along with 13 federal

agencies and academic representatives collaborated to make the changes to the list of IT management knowledge and skills required for all federal government CIO staff.

“Records management is a key competency for IT managers and with the recent issues regarding personally identifiable information it even becomes that more critical,” says Barry C. West, Chief Officer and Co-Chair of the IT Workforce Committee.

The CIO Council and its IT workforce committee is committed to developing and maintaining an effective IT workforce by encompassing the full employment life cycle, focusing on planning, recruitment and retention. With the government streamlining more IT resources, creating more enterprise-wide programs, they must ensure that the workforce is well versed and trained to execute their programs with little risk.

For more information please visit: www.cio.gov

About ARMA International

ARMA International (www.arma.org) is a not-for-profit professional association and the authority on managing records and information. Formed in 1955, ARMA International is the oldest and largest association for the records and information management profession with a current international membership of more than 10,000. It provides education, publications, and information on the efficient maintenance, retrieval, and preservation of vital information created in public and private organizations in all sectors of the economy. It also publishes the award-winning Information Management Journal.

MER '07 PROGRAM ANNOUNCED

Cohasset Associates, Inc. is pleased to announce the program for the 2007 National Conference on Managing Electronic Records (MER '07).

DATE: May 21 - 23, 2007 for the conference, May 20th for the pre-conference tutorials.

LOCATION: Chicago, Illinois at the Westin Michigan Avenue Hotel

SPECIAL FEATURES

KEYNOTE ADDRESS – A special two-part presentation by Karen Strong of Clarity - together with an “A” Team of Compliance, Records Management, and Technical professionals.

Keynote Part 1

This interactive MER '07 Keynote introduces a framework for Enterprise Content and Records Management (ECRM) process improvement. Karen Strong will define the organizational processes that contribute to the attainment of legal, operational, and technical goals.

Every audience member will participate, through a real-time data capture system, to demonstrate the value of knowing ‘your ECRM number’.

This first part of the MER '07 Keynote will provide you with the information foundation for Wednesday's second part of the Keynote - where the concepts presented in this session are applied in an innovative and insightful case study.

This year's two-part MER Keynote session will change the way you think about enterprise content and records management.

Keynote - Part 2

The Enterprise Content and Records Management (ECRM) process model introduced in the opening Keynote session on Monday will have established a standard approach for improving the processes that contribute to the attainment of legal, operational, and technical goals.

In this Second part of the MER Keynote, the cross-functional communication and collaboration necessary to accomplish your organizational objectives and improve your ECRM number will be discussed. The highlight of this second part of the MER Keynote will be presentations by an “A” team of experienced industry experts detailing their roles and the processes they used in the development of this innovative and practical approach that will accelerate the successful management of electronic records.

This year's two-part MER Keynote session will change the way you think about enterprise content and records management.

CASE STUDIES

Learn from the experiences of the leaders of ERM implementation:

- Altria (Compliance & ERM training)
- Central Intelligence Agency (Managing Electronic Records: “Hurry up and LISTEN!”)
- ConocoPhillips (e-Records Holds: Preserving e-Records and ESI)
- National Archives of Sweden (Total Cost of Ownership)
- National Archives and Records Administration NARA (Searching Techniques: The Next Contested Area in Discovery)
- Microsoft (The ERM functionality of Office 2007)
- Philip Morris International (Automatic Retention of e-Mail for Litigation Purposes)
- United States Patent & Trademark Office USPTO (Searching Techniques: The Next Contested Area in Discovery)
- Valero Energy (Keynote Address Part 2)

CONFERENCE PROGRAM

The MER '07 Conference program will include:

- 39 outstanding speakers
- 26 informative sessions
- 16 leading solution providers
- 4 in-depth all day pre-conference tutorials
- 2 special Keynote Addresses

Opening Keynote

Closing Keynote

NETWORKING

There will be three of the MER's highly successful Networking Receptions: Sunday, Monday and Tuesday.

FREE AUDIO CDs OF EVERY SESSION

In addition to their conference notebook, every registrant will receive a complimentary audio CD of all the sessions, so every attendee will benefit from all the information provided in every session.

SPECIAL PRE-CONFERENCE TUTORIALS

Four outstanding 6-hour tutorials, conducted by renowned experts, will be held on May 20th:

- e-Mail Management...or Mis-Management???
- Charting the Path to Enterprise Content Management: Strategy, Methodology and Architecture"
- Microsoft's 2007 Electronic Records Keeping Capabilities: How to Put Them to Work for You
- Assured Records Management: Align ERM Performance to Business Strategy

EXHIBITORS

In addition to the conference program, MER attendees will have an opportunity to meet with the 16 Select Solution Providers who will be exhibiting in suites at the conference hotel.

COMPLETE CONFERENCE INFORMATION

Full details about the MER '07 conference program are available on the web site www.merconference.com

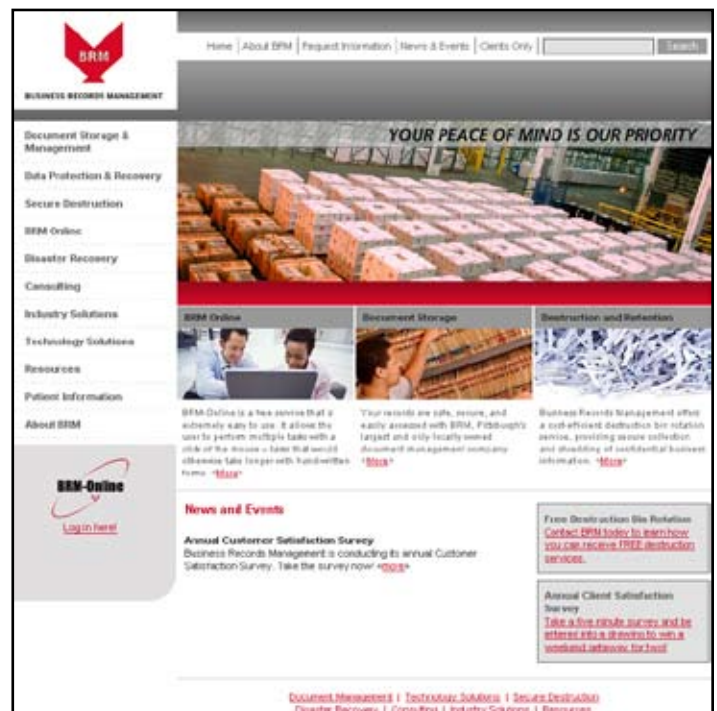
BRM Has a Brand New Website!

After months of hard work and anticipation, Business Records Management is excited to announce our brand-new website, www.businessrecords.com. The site features a completely new layout, sharper colors, easier navigation, and a crisp look. It is designed to give visitors easy access to information on what BRM has to offer, as well as provide customers with additional resources like BRM-Online, current news & events, and more.

Visit the site today, and look around. You will find a number of features, including:

- Detailed Service Information.
- Easy Access to BRM-Online.
- Customer Satisfaction Survey
- Regulatory Compliance Resources
- E-Newsletter.
- Directions to all of our locations, using Google Maps.
- News & Events section.
- "Meet Our Team" page.

As always, we appreciate all of your questions, comments, and suggestions regarding the site. Please e-mail BRM Marketing Assistant Josh Madore at marketing@businessrecords.com. *Enjoy!*



Employee Profiles



Debbie Curry joined the BRM family in January 2007, as the HR Specialist. Her duties include benefits administration, recruiting, interviewing, workers comp issues, and other special projects. Debbie enjoys helping

BRM employees by answering any questions they may have with her knowledge of human resource issues. She considers obtaining her BS/BA degree from Robert Morris University her greatest accomplishment in life. When she's not working, Debbie loves to vacation with her husband Tom in Las Vegas or any tropical Island.

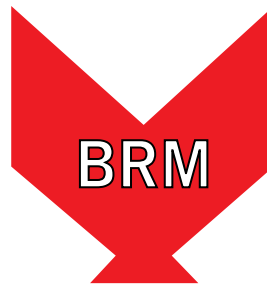


Kevin Gillespie also joined BRM in January 2007. He is the newest Sales Executive in Pittsburgh. Kevin brings his excellent networking abilities and friendly personality to his job of meeting prospective clients

and closing deals. He is particularly proud of graduating from Grove City College in three years, and enjoys vacationing in Mexico. In his spare time, Kevin is busy producing music for artists under his own record label, snowboarding, and relaxing with his girlfriend Tina.

Congratulations eNewsletter 1st Quarter Winners

Congratulations to **Mr. Paul Myers** of Matthews International Corporation, and **Ms. Monica Gulyban** of Allegheny Intermediate Unit. They both received a \$50 retail gift card. On behalf of everyone at BRM, thanks again and we hope you have a great time shopping!



**BUSINESS RECORDS MANAGEMENT
BRM Disaster Recovery Services, Inc.**

1018 Western Avenue
Pittsburgh, PA 15233

Voice: 412.321.0600

Fax: 412.321.5152

Web: www.businessrecords.com