



National Archives News

The Newsletter of the Archives and Records Management Unit

June, 2008

Vol. 2 No.6

Disaster Management for Records



This is a Hurricane Disaster! How Prepared are You!

Disaster Management Tips for Records

Please pull out your Disaster Management for records pamphlet and follow the guidance there. Here are a few reminders:

- *Everyone should observe the general precautions outlined in the Disaster Management Handbook.*
- *Each office should revise its 'response team' and should know who is responsible for doing what if and when disaster strikes*
- *Examine all rooms where records are stored and check for leaks*
- *Know where fire distinguishers and sprinklers are located*
- *Ensure that officers know how to use fire-extinguishers*
- *Store books, documents, records off the floor in basement storerooms*
- *Store plastic sheeting for covering stacks of shelves and documents*
- *Store bags of sand to check floor water in basement storerooms*
- *Check and restock the list of precautionary supplies*

History Teasers

- 1. In what year was the wreck of HMS Nymph found in Road Harbour?*
- 2. How many members were elected to the House of Assembly in 1773?*
- 3. Who was the President of the Virgin Islands in 1741?*
- 4. Who was the Member for Trade and Production from 1950-1957?*

Answer all four correctly and win a prize. Contact the Archives and Records Unit

Out reach: Community Awareness and Involvement

Records May Day was a success with several members of the public visiting the Unit for the first time, viewing the RM video and microfilmed records and asking interesting questions. Each took away an acid-free box or envelope to assist in managing their records at home. However, many more telephoned instead, some with requests for advice on preserving their records and with their research.

Visits to Schools and Churches: The inspection of Churches and Schools records by the Chief Records Management Officer is turning up many valuable records, which for the most part are 'at risk.' So far seven churches and seven schools were visited. Storage of many is unsatisfactory and needs urgent remedying. Advice is being given on the spot but at the end of the exercise a Report with recommendations will be submitted to the Ministry and Department Of Education and Culture.

Interactive Research on Virgin Islands shipwrights, boats, captains and sailors is continuing. Persons are reminded to call in any pertinent information.

Records Management Education

The Government Archivist conducted workshops in the Junior and Senior Induction Training Programmes for Civil Servants sponsored by the Training Division during March and April 2008. He also held remedial seminars with three Government departments.

Two trainers from Professional Microfilm Firm (PR), held demonstrations of micrographic equipment at the Unit

Appraisal Workshops are due to be held for Records Officers during the second week in August. Actual dates will be posted in the July Newsletter.

Industry News

Outside email accounts in the workplace: How safe?

Companies may have the most secure corporate e-mail system possible, but that means nothing when it comes to the very real risks to the organization when employees forward their office e-mail to free web-accessible accounts from such providers as Google, Yahoo and MSN.

Employees often forward their work e-mail – some of which may contain sensitive company information – to their personal accounts, bypassing any password requests meant to protect them.

Experts urge organizations not to disregard the danger. They warn of corporate secrets leaking from the well-protected corporate network with a click of the “forward” button and fear that forwarding e-mails might inadvertently expose proprietary information.

Corporate networks usually have several layers of protection against hackers, including special software and multiple passwords. Web-mail systems, however, have weaker security and could allow viruses or spy-ware to get through, meaning employees accessing these systems from the office could accidentally download bugs and infect the entire corporate network, according to a *N York Times* report.

Another risk, the *Times* noted, is that employees’ use of outside e-mail may result in companies being unable to comply with legal rules requiring them to archive corporate e-mail, which is discoverable in the event of a lawsuit, because messages sent from outside e-mail accounts do not pass through the corporate network.

Along those lines, many technology professionals worry that Google and other web-e-mail providers may actually own the intellectual property in the e-mail that resides on their system, according to the *Times*. Gmail’s terms of service, however, states that e-mail belongs to the user, not to Google, and the *Times* reported that the company’s extensive privacy policy ensures no human at Google reads user e-mail.

In an attempt to fully protect themselves, though, some companies have gone so far as to ban employees from accessing outside e-mail in the workplace. And, according to e-mail security firm Proofpoint, 37 percent of U.S. firms surveyed said they monitor employees’ use of web mail.

(From: *You’ve Got Mail and Trade Secrets* IN *Information Management Journal*, Vol. 41, No.3)

Protecting Information from Insiders

Although organizations are making strides in protecting their sensitive information from outsiders threats, reports show they often are failing to protect it from the much greater threats posed by their own employees.

In recent months, insider data theft stories have been grabbing headlines from tales of stolen laptops. Despite the growing risk, however, many businesses – even the biggest and most well known – are not properly protecting their sensitive information from inside threats. For example, a federal jury recently convicted a former Coca-Cola secretary of conspiring to steal trade secrets from the world’s biggest beverage maker in an effort to sell them to competitor Pepsi Company. Joya Williams faces up to 10 years in prison, pending sentencing.

In February, Computerwork.com reported that a cell development technologist at Duracell Corp. admitted to stealing research related to the company’s AA batteries. He e-mailed the information to his home computer and then forwarded it to two Duracell rivals.

In another case, a former DuPont scientist walked away with more than \$400 million worth of trade secrets after being hired by a rival company. Gary Min, who had worked at DuPont for 10 years, pleaded guilty to stealing proprietary data from DuPont by illegally down-loading or accessing thousands of documents stored in an electronic library. He faces a maximum of 10 years in prison and a fine of up to \$250,000.

Experts say too many firms are still relying on the old security model that advocated protecting information assets from the outside in through firewalls, intrusion detection systems, and other defenses. But those methods will not protect companies from insider threats.

“Frankly, we all have to actively stop thinking of insider vs. outsider” and improve access controls for all users,” Matt Kesner, Chief Technology Officer at California law firm Fenwick & West LLP, told Computerweek.com. “It means looking at each and every person and machine as an island and deciding what rights and access each person and machine needs or doesn’t need.”

Paying closer attention to access rates would have provided DuPont a clear warning about the jeopardy of its intellectual property. According to court data, Min downloaded about 22,000 documents abstracts from DuPont’s Electronic Data Library server and accessed another 16,700 full-text PDF files, the documents related to DuPont’s major products and technologies, including some that were in the research and development stage. Min illegally downloaded and accessed more than 15 times as many documents as the next highest user of the DuPont database, according to Computerworld.com. Still, he wasn’t caught until after he left the company.

Upon Min's registration, an internal investigation exposed his activities, which DuPont then reported to the FBI and the U.S. Department of Commerce. Meanwhile, he was brazen enough to upload another 180 of DuPont documents onto a laptop – owned by Victrex PLC, the England-based company which he left DuPont to join a full month after. DuPont contacted Victrex officials, who seized Min's laptop and turned it over to the FBI. (Nikki Swartz IN Information Management Journal, Vol. 41, No.3)

Feedback

The Archives and Records Management Unit took centre page coverage in the ACARM Newsletter, Issue 41, published by the Association of Commonwealth Archivists and Records Managers, in London, UK. The Editor specifically prized the Old Pictures Exhibition held at the Central Administration Complex last year.

Some Comments on Records May Day:

For research on the family of Salt and Peter Islands, good!

"Very interesting!" Keep up the good works".

"This is touching. God is good!"

"The Open House idea is a good one."

"Thanks for the acid-free box!"

Quote for Today

"The average life of a piece of digital information is 5 to 7 years. Vital government information is now becoming unreadable or even unrecoverable because the media on which it is stored is deteriorating. Digital files need active management to ensure that they remain readable over the long term". ... Kelvin Smith, Consultant UK

Friends of the National Archives

There will be a Friends meeting on June 25th at 4.00 pm., at Conference Room # 10, Central Administration Building. Interested persons are invited to attend.

Virgin Islands National Archives, Archives and Records Management Unit, Deputy Governor's Office, Burhym Bldg, 49 deCastro Street, Tele: 494 3701 ext 3044/ 2562/2365. email: vpenn-moll@gov.vg Website www.dgo.gov.vg