# Information Security Updates

## Data Leakage Prevention

### Security Incident

**Calgary Medical Clinic System Hit by a Virus**

On 17 March 2010, numerous patients associated with a clinic of University of Calgary, namely Sunridge Medical Clinic at Calgary, Alberta, Canada, are being cautioned that as a computer virus exploited a medical database, there is a possibility that their personal health details could have been compromised.
(http://www.spamfighter.com/News-14096-Calgary-Medical-Clinic-System-Hit-by-a-Virus.htm)

### Statistical Report

**Threats Report Q4 2009**

McAfee Labs observed numerous SQL-injection attacks aimed at vulnerabilities in web server applications. Due to their popularity, Adobe Flash and Acrobat Reader are a huge target for hackers looking for weaknesses in client applications.
(http://www.mcafee.com/us/local_content/reports/threats_2009Q4_final.pdf)

# I. Background

### Case Study

**Personal information stolen for millions of student loan recipients**
The company Educational Credit Management Corporation reports that the personal information of 3.3 million federal student loan borrowers has been stolen, including names, addresses, birth dates and social security numbers. A portable medium containing students' personal data was stolen on 20 March 2010.
(http://www.scmagazineus.com/info-about-33-million-student-borrowers-on-stolen-device/article/166810/)

Campus networks are at greater risk to breaches because they must be open, carry a lot of data, and have many access points (mobile devices, computer ports, personal e-mail and instant messaging). All campuses should be vigilant regarding their data breach prevention policies, personnel and solutions.

One of the solutions to mitigate risk of data loss through portable media as shown in the case above is to implement Data Leakage Prevention (DLP) tools which can prevent sensitive data to be transferred to portable devices, as well as external locations through the network.

### Data Leakage Prevention (DLP)

Data Leakage Prevention (DLP) tools are systems that identify, monitor, and protect data in use (e.g. endpoint actions), data in motion (e.g. network actions), and data at rest (e.g. data storage) through deep content inspection and with a centralised management framework. These systems are designed to detect and prevent the unauthorised use and transmission of confidential information. Currently, there are three main types of DLP design:

- **Network DLP –** Network DLP tools crawl through network and fingerprint sensitive files and records. They will detect if a particular important file or dataset is being transferred somewhere through the network. However, network DLP technologies do not have the capacity to monitor data that are locally managed at an endpoint, such as personal e-mail and mobile device. It is difficult to thwart insider threats if the endpoints are not guarded.
- **Endpoint DLP –** These are agents or client software that reside at endpoints, such as mobile devices, computer ports, personal e-mail and instant messaging. They can detect if an important file is being transferred out from the endpoint. They log, block and notify actions that violate security policies.
- **Embedded DLP –** Embedded DLP are customised tools which are embedded within individual application system, such as email system and Adobe reader for the purpose of protecting specific information, e.g. restriction of copying and printing of documents.

Footnote 1:
http://www.fujitsu.com/downloads/MAG/vol46-1/paper13.pdf

**Latest Updates**

### OneLock Thwarts Data Leakage via USB Storage Devices

The University of Hong Kong (HKU) is pleased to share a proven, practical and powerful solution – OneLock – to combat data leakage. It offers an unprecedented level of data protection for any off-the-shelf USB storage devices. (http://www.cecid.hku.hk/pressrelease_20100317_OneLockThwartsDataLeakage.php)

**Major Outbreak**

### World Cup phishing

The biggest event for sports fans around the world is the FIFA soccer World Cup. With the recent announcement of the final draw for the games that will take place in South Africa in June and July 2010, interest in the event and how to obtain tickets is now in full swing. Opportunistic cybercriminals have started distributing World Cup–themed phishing scams to trick fans out of their sensitive information. (http://www.spamfighter.com/News-12925-FNB-Warns-of-2010-FIFA-World-Cup-Phishing-Scam.htm)

# II. General Users

### Roles and Responsibilities

General users of the computer resources at campus have an important role to data leakage prevention. Being part of the campus network, all end users have the obligation to protect data in the campus network. Below are some good practises for managing information and data:

### Good Practices for general users to prevent data leakage

1. **Turn off unused Wireless Network** – Disable the Wireless Network Interface Card when connection to the wireless network is not required. This will prevent attacks that are performed through the Wireless Network Interface Card.
2. **Encrypt your files** – Make use of data encryption software such as WinZip (http://www.winzip.com/index.htm) as well as TrueCrypt (http://www.truecrypt.org/) for file encryption. A strong key, created in line with the security policy, should be used for encryption when files are being transferred into removable media or through email. Encrypted USB storage device may be used for additional level of protection.
3. **Avoid sending sensitive data over Internet email** – Use your campus email to send confidential information. Sending sensitive information over an Internet email may result in a copy of your sensitive data being stored or archived by a third-party server.
4. **Store your data on a secure network drive** – Store your data on the server instead of the hard drive of your own laptop to prevent data leakage should you lose the laptop.
5. **Virus scan over files from external source** – Scan the files you downloaded from the Internet, whether it is an email or an external storage device before you open or save the file. Virus scanning is important to prevent data leakage.
6. **Ensure proper security is enabled for computer** – Be responsible for protecting the security of your computer. Loss or theft of a computer, USB storage device or even printer, is a common cause to the loss of important data.
7. **Do not leave your printed documents unattended** – Remember to collect all the printed documents from the network printer and ensure all print jobs are completed when you leave.

**Related Incident**

### Bogus Intranets Scam University Students

Security Company (RSA) has detected a sudden rise in targeted attacks on US universities - particularly public state institutions - against internal websites used to serve students with services such as webmail. Such servers often contain personal data such as grades, names, addresses, and payment information. (http://www.cio.com/article/569964/Bogus_Intranets_Scam_University_Students)

**Related Article**

**Nine out of 10 firms use data leakage prevention tools**

Ninety-three per cent of businesses use data leakage prevention (DLP) tools, according to interim figures provided by the Launchpad Europe IT Security Index 2009. 70% of businesses worldwide are planning to make investments in DLP this coming year.
(http://www.computerweekly.com/Articles/2009/10/14/238136/Nine-out-of-10-firms-use-data-leakage-prevention-tools.htm)

**Statistical Report**

**2009 Data Breach Investigations Report**

The Data Breach Investigations Report (DBIR) is an annual publication based on cyber crime cases. The report covers the indicators, mitigation strategies, and impact of the most common attack types.
(http://www.verizonbusiness.com/resources/security/reports/rp_2009-data-breach-investigations-supplemental-report_en_xg.pdf)

**Legislative Update**

*There are no updates in this section.*

# III. Management

Security is not just implementing a tool or an IT Department issue. Management needs to understand there are three components to security, which are people, process and technology. A good information governance framework is an essential element for the implementation of data loss prevention programme in addition to DLP technology implementation.

**Fundamental aims of Information Governance:**

- To support the provision of high quality care of data by promoting the effective and appropriate use of information
- To encourage responsible staff to work closely together, prevent duplication of effort and enable more efficient use of resources

Campuses need to be vigilant yet realistic regarding their data breach prevention policies, personnel and solutions. The following best practices may help:

1 **Conduct a Risk Assessment** – Understand what type of information are the most sensitive, who might expose it, how and where it could be exposed, and what applications use it.
2 **Categorise the Data** –Identify and categorise appropriate level of security on various types of facilities, such as "confidential, restricted and public".
3 **Determine who has access** – Determine who has access to various types of data, and access should be granted on a need-to-know basis.
4 **Take a Multi-Layer Approach**
   - Implement the Data Leakage Prevention (DLP) tools to prevent data loss through network, end users as well as applications.
   - Make use of different safeguards such as firewalls, anti-virus & anti-spam software, intrusion prevention (IPS), network access control (NAC) and possibly IP white lists to strengthen the IT environment of the campus.
   - Controlling the administrator rights of a computer reduces the chances of an insider intentionally or unintentionally downloading the malware or malicious code.
5 **Other relevant controls** – Consider implementing additional data protection controls such as data encryption, removable media tracking, physical access, and secure data disposal. Click "Read More" for further reference.

Read More [2]

**Related Incident**

**Student information was part of security breach**

According to Liz Latt and Beth Fortune in Public Affairs, a professor's desktop computer who kept a database of his grade book, containing the names and social security numbers of 7,174 current and former students, was stolen some time during the weekend of Feb. 6 2010.
(http://www.scmagazineus.com/stolen-vanderbilt-university-desktop-contained-students-personal-information/article/166064/)

Footnote 2:
http://www.campussafetymagazine.com/Articles/?ArticleID=189