HealthManagement
Promoting Management and Leadership

Volume 2 / Issue 3 2007 - Management

Of Disaster and Data Managment

As computers become ubiquitous, the issue of vital data loss due to disaster, is a growing concern for all computer users – from individuals and small firms, to large organisations in sensitive areas such as the military, banks or hospitals and, of course, healthcare facilities.

Such security concerns sweep across a vast range of possibilities: the theft or loss of physical assets such as computers, the possibility of viruses and Trojans in IT systems, or fire, natural disasters and lightning strikes.

In June 2006, the newspaper USA Today reported the findings of a survey by Carbonite, a Boston-based firm, of 185 self-described 'business-savvy' people. 69% of the respondents said they had lost data due to accidental deletion, disk or system failure, viruses, fire or another disaster. 40% said they had lost data two or more times in the previous year. Globally, the cost of such losses can be estimated in the upper tens of billions of dollars.

The Scenario in Healthcare

In the healthcare field, protecting confidential patient information is more critical than ever as more data moves from paper to computers and is then made available online.

The best-known scandals in such contexts have been in the US: most recently, in the shape of an Internet posting in March of the names and medical records of 2,000 patients at Rhode Island's Westerly Hospital, or the theft of an unsecured laptop last year with similar data on over 350,000 patients of Providence Healthcare, which operates hospitals in the western US.

Such situations cannot be ruled out in Europe. However, it is true that the US is less stringent about protecting private information, unlike the EU, where the Data Protection Directive has forced companies and institutions to take security more seriously – to avoid being punished for privacy violations. Indeed, one shape of things to come was a near- GBP 1 million fine imposed last February by the Financial Services Authority on British Building Society Nationwide, after a laptop containing sensitive customer data was stolen from an employee.

The Explosion in Data Generation

For many healthcare IT managers, however, the cost of data storage and security remains an issue. So too does the unremitting growth in data volumes. One EU hospital IT manager told Healthcare IT Management that data has begun to "literally explode" at his facility. This would become a "major issue in the coming years", especially as e-Health programs began to go live. He however had found it a hard case to make to his CFO about the limitations of their 2nd generation disk/tape backup; "buy some more tapes", was the response.

Indeed, according to a March 2007 report from IT industry analysts IDC, digital data creation over the next four years is set to increase sixfold – from 161 exabytes in 2006 to 988 exabytes in 2010 - and have major consequences for IT departments. Businesses and organisations, on their part, would be responsible for the security, privacy, reliability and compliance of around 85 percent of this.

As a result, IT managers would "see the span of their domain considerably enlarged."

On its part, industry has been seeking to move to provide state-of-the-art, but realistic choices – although some of the cutting-edge solutions remain expensive because of low demand.

Remote storage vendors, for instance, already deploy specialised tools to gather data from remote servers, compress and encrypt it, and then transfer it offsite. Technologically, as part of their online backup to clients, some provide not only sophisticated data compression – but also, more recently, tools to detect data changes at the block level – saving common files and unique data just once. This caps the speed of growth of data, and also reduces data transfer and storage requirements up to threefold.

E-Health and Data Growth

The IDC report mentioned above noted that around one-fifth of the extra data generated last year was a result of new compliance rules and laws such as Sarbanes-Oxley and Basel II. Though these focus on corporations and financial institutions, it is not too difficult to draw parallels about new e-Health regulations providing exactly such an escalation in data creation. Indeed, a study by Accenture in 2005 already pointed to a spike in digital data arising simply from the use of RFID devices (which remains a priority for modernising hospitals).

In the face of this, it is clear that proactive, strategic thinking by hospital CEOs and CFOs on data storage – within the framework of security and disaster prevention - needs to become a priority.'

Published on : Mon, 31 Dec 2007