TOSHIBA GIỚI THIỆU THẺ NHỚ SD... 8GB

Toshib

Toshiba dự định tung tiếp một "quả bom" vào năm tới, một chiếc thẻ Secure Digital (SD) có dung lượng choáng váng tới 8GB, tương đương với 2000 bài hát hoặc 2500 bức ảnh chụp bằng một camera số 6 chấm.

Với kích thước chỉ xấp xỉ một con tem bưu điện, thẻ SD đang được sử dụng rộng rãi trong các thiết bị điện tử cầm tay, từ máy ảnh số cho đến camcorder và PDA. Điều làm nên sự độc đáo cho loại thẻ mới của Toshiba, ngoài dung lượng "khủng" của nó, còn là khả năng ghi được dữ liệu với tốc độ lên tới 6 Mb/giây.

Với tốc độ đó, loại thẻ mới hoàn toàn thích hợp với camera cao cấp như Panasonic HDC-SD1 1080i, vì những thiết bị này thường thu dữ liệu trực tiếp lên thẻ.

Tên khủng bố tí hon?

Nguồn: Sdcard.org

Tuy loại thể mới rất gây ấn tượng, song nó cũng có thể khiến các Giám đốc thông tin, người phụ trách trung tâm dữ liệu đau đầu trong việc bảo vệ mạng thông tin tuyệt mật của mình trước nhân viên "hai mang".

"Nguy cơ tay trong đã gia tăng mạnh vài năm gần đây", chuyên gia Khalid Kark của Forrester cho biết. Kark tin rằng nguy cơ từ những công cụ lưu trữ dung lượng lớn, di động kiểu này chắc chắn cũng leo thang theo trong thời gian tới.

"Cụ thể hơn, chúng ta đã thấy được mặt trái của những chiếc ổ USB. Các doanh nghiệp rất khó

quản lý vấn đề này vì làm sao mà quản cho xuể những chiếc ổ USB bé tí tẹo mà ai cũng có thể giấu trong người".

Quả thật, ổ USB, thẻ SD, thẻ Compact Flash, thẻ Memory Sticks không thể tách rời khỏi những thiết bị thiết yếu với cuộc sống con người hiện đại như ĐTDĐ, smartphone, máy nghe nhạc MP3... Không ai có thể cấm nhân viên mang những thiết bị này vào phòng làm việc.

Với một chiếc thẻ 20 USD, bất cứ một nhân viên quèn nào, nếu có ý định, cũng có thể rút được hàng ngàn, hàng triệu tên khách hàng, số điện thoại, ngày sinh và tệ nhất: tình trạng sức khỏe hoặc dữ liệu về thẻ tín dụng của họ.
Rò rỉ thông tin

Nhằm đáp lại nguy cơ này, một số doanh nghiệp đã triển khai cài đặt phần mềm chống rò rỉ thông tin (ILP). Phần mềm này chuyên theo dõi mạng nội bộ, phát hiện và phong tỏa các công cụ lưu trữ đang kết nối trái phép vào hệ thống.

Theo chuyên gia Kark, một số phần mềm ILP thậm chí còn có thể phân biệt giữa các dữ liệu nhạy cảm và thông thường, phân bổ quyền truy cập cho các người dùng khác nhau tùy theo mức độ nhạy cảm của thông tin.

Kết quả ư? Nếu trong quá khứ, các hãng luôn bị ám ảnh với việc thứ gì sẽ "nhảy" vào mạng của họ - virus, spyware, malware thì giờ đây, họ chỉ lo những thứ gì sẽ bị lọt ra ngoài mà thôi.

Trọng Cầm