

DeltaCrypt Technologies Inc.

261A Epinettes
Piedmont, Qc, Canada, J0R 1K0
Phone (450) 227-6622
www.deltacrypt.com

White Paper: How Can DeltaCrypt DUSK Suite Prevent «Wikileaks Scandals»?

DeltaCrypt DUSK Suite Solution

The **DUSK Suite** prevents illegal intrusions as well as data leakage by increasing knowledge on network activities such as files being copied out. It monitors authorized and unauthorized devices connected to a network to help better identify vulnerable workstations or simply to warn on unusual activities. Notifications are log recorded or sent out by email to get your Administrator's immediate attention. Finally, the **DUSK Suite** lets organizations silently take an integral copy of file content leaving your premises should one need to access or verify file contents.

Contents

DeltaCrypt DUSK Suite Solution	
Introduction	2
Could Wikileaks scandals have been prevented?	3
Security Environment before Wikileaks scandals	3
DeltaCrypt DUSK Suite Solution	3
Implementation	4
Summary	4

Introduction

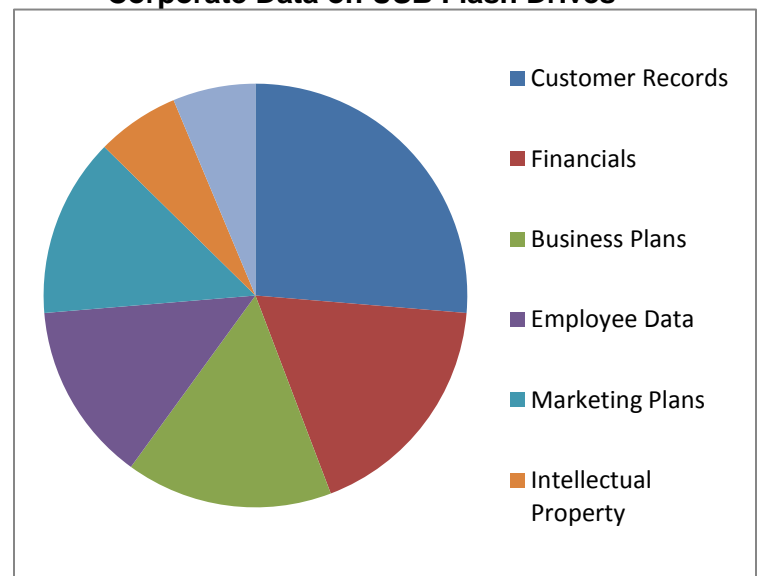
The recent chapter of data leaks from Wikileaks proves once again that in an age of web-based social networking and micro blogging, cloud computing, computers thinner than a magazine, smart phones that carry the office wherever you are and USB drives that store more data than you can supply, that nothing more remains secret.

But are big and small businesses doomed to be big brothers with their employees so they can stay protected or should we just sit back and consider this as a sign to just not be evil?

Today's nature of doing business and research is that people look for competitive edges over others.

A survey conducted by Sandisk in 2008 indicated that data files most likely to be copied to a personal flash drive included the following:

Corporate Data on USB Flash Drives



Could it be simply pure curiosity?

What is clear is that when it comes to business and organizations- everyone has something to hide. What they don't realize is that 'everyone has something to protect' too. Data should always be respected.

So what can you do in order to keep data secure?

Could Wikileaks scandals have been prevented?

According to a Wired article, Manning, an army intelligence analyst, revealed that his methodology for exporting classified files was a classic case of deflection-by-Gaga. "I would come in with music on a CD-RW labelled with something like 'Lady Gaga', erase the music then write a compressed split file. No one suspected a thing and, the odds are, they never will. [...] [I] listened and lip-synced to Lady Gaga's 'Telephone' while exfiltrating possibly the largest data spillage in American history."

This insider's job done by a 22-year-old baby-face private clearly indicates that your biggest threat most often comes from the inside. In addition, a recent PGP survey indicated that data breaches involving malicious or criminal acts are much more costly to organizations than incidents resulting from negligence or system glitch.

We are all aware that the most negative cost impact results from the diminishment of confidence and trust in the breached company.

Security Environment before Wikileaks scandals

Enacting Security Policies

By enacting security policies, one can optimistically believe that all users will obey by the rules and will never be tempted to eavesdrop or to read sensitive data they are not authorized to.

Know Your Employees Well

Management can positively believe that by verifying references, checking profiles,

obtaining security clearances it would guarantee employees' loyalty. In the last Wikileaks chapter, not only was the source a military private, but he was part of army intelligence with all the proper authorizations and clearances! Can we be ensured that trust always leads to loyalty?

Implement Access Control

Security in the operating system controls the use of system and network resources through the interrelated mechanisms of authentication and authorization. After a user is authenticated, the system then determines if an authenticated user has the correct authorization to access a resource. But wasn't the Wikileaks source properly authorized to access the sensitive data?

DeltaCrypt DUSK Suite Solution

DUSK Suite protection lets you benefit from state-of-the-art mobile device protection as well as mobile device control with audit and tracking capabilities. No more concern about securing new devices, devices that were lost, or simply devices to be eventually replaced.

Log Reporting

DUSK Suite provides information on mobile device activities to better identify vulnerable workstations to illegal intrusions. To prevent data leakage, it also records logs on files leaving your network on DUSK-USB protected devices. It gives information on who had access to what, when, and from which user account and computer.

Alerts

The DUSK Suite is also designed to detect and to prevent the unauthorized use and the copy of confidential information onto DUSK-protected USB sticks or hard drives. By controlling the file formats or the file volume, your network administrator may be notified of such activities with log alerts or by receiving email alerts. The shadow copy function enables integral access to file content leaving your network.

FIPS 140-2 Certification

DeltaCrypt technology is FIPS 140-2 validated level 1. The Federal Information Processing Standard--FIPS-- Publication 140-2 is a U.S. government computer security standard for accrediting cryptographic modules.

Custom-Built Solution

Don't let your organization's special requirements keep you from protecting or controlling sensitive corporate data. The DUSK Suite can be tailored to your needs and environment.

Implementation

On the client side, the DUSK Suite can be pushed using GPO or SMS and is configured with MS Active Directory.

On the server side, the Administrator Module may be installed on any computer. This module is used for DUSK Suite administrative tasks such as creating administrator's recuperation keys or displaying log reports.

Summary

We value mobile computing devices for the flexibility and convenience they provide, but mobility presents significant challenges for IT administrators charged with keeping their companies data and networks secured. What's more, the regulatory climate in which companies must operate is placing a greater demand on the control of corporate data. While these challenges make managing security on mobile devices a trickier proposition, with DUSK Suite, administrators can help plug the holes that mobile devices have a way of opening in company's security infrastructure.

With the DUSK Suite transparent control running on users' workstations, users will be prevented from contravening corporate security policies. The DUSK Suite audit and tracking capabilities enables organization to perform better external and internal risk assessment. It allows organizations to implement the necessary constraining measures in a timely manner to keep prying eyes from leaking sensitive data.

DeltaCrypt believes that by combining prevention with protection, the DUSK Suite is best-suited to answer any corporate mobile security needs.

