



Stolen Drives and Servers

Don't Think it Can't Happen in Your Data Center

September 2007
Trusted Strategies LLC

John R. Muir
Managing Partner





Stolen Drives and Servers

Don't Think it Can't Happen in Your Data Center

September 2007

Executive Summary

Almost every organization is well aware of the risk to confidential data stored on mobile devices such as notebook PCs that can be lost or stolen. But few organizations realize that drives or even entire servers are vulnerable to theft, loss, or maintenance mix-ups despite the “protection” of residing in the organization data center. Of course, that means that the confidential data stored on those devices is subject to unauthorized use by the growing army of cyber criminals. Because data centers contain the most concentrated data in the organization, such thefts can be catastrophic in terms of financial, regulatory and legal consequences. Even small incidents can necessitate high costs of remediation because when such thefts occur it is extremely difficult to determine what was compromised, so the “worst case” scenario must be assumed.

Background

The theft of a single notebook PC is now understood as a potentially disastrous event. In recent years there have been dozens of reported incidents involving millions of compromised records in both the government and private sectors. This trend is due not only to an ever increasing percentage of mobile PCs used in the workforce, but also to the economic pressure to push vital data to the edge of the enterprise.

The obvious risks associated with mobile devices have triggered a large increase in enterprise PC security products, most notably full disk encryption products that automatically and transparently secure everything written to the hard drive. This is largely because encryption has become the preferred method of complying with the growing body of state and Federal regulations that require the confidentiality of private information to protect individuals and public enterprises.

Strangely, however, when it comes to protecting data on servers and drives in the data center, most organizations tend to overlook encryption and instead rely on physical security measures such as guards, door locks, and video cameras to prevent equipment from “walking out the door”. Even then, physical security as a means of preventing data loss generally receives much less attention than the prevention of data theft by remote intrusion. Hence many companies that provide the latest in firewalls, user authentication systems, intrusion prevention systems and vulnerability management systems may grow lax in preventing the physical theft of servers and drives that contain essential, confidential information.

Reality Check: Servers and Network Drives Are Frequently Stolen

Multiple published reports serve notice that confidential information stored on data center devices is at risk not only from remote hacker attacks, but also from physical theft or loss. Consider these recent examples:

- A thief stole a computer server belonging to American Insurance Group (AIG), putting the personal data of nearly 1 million people at risk. The computer server contained personal electronic data for 930,000 Americans, including names, Social Security numbers and tens of thousands of medical records.
- The Transportation Security Administration (TSA) is missing a hard drive containing some 100,000 current and former employee payroll records. The missing data contains names, Social Security numbers, payroll information, bank account and routing information.
- A theft of computer hard drives from TriWest Healthcare, a government contractor, exposed the Social Security numbers and other personal records of 500,000 military service members and their families in 16 states.
- More than 180,000 customers of a Canadian insurance company have been warned about possible identity theft after a computer hard drive containing personal information was found missing from an IBM subsidiary.
- A computer hard drive with sensitive information was stolen from the Birmingham (Ala.) Veterans Administration Medical Center. A file on the portable hard drive had billing information for 1.3 million doctors and included information on more than 500,000 war vets.
- Four hard disk drives containing information on over 15,000 soldiers were stolen from Fort Carson. The hard drives stored critical information including social security numbers.
- Two men posing as computer technicians stole two mainframe servers after they tricked their way into the Sydney Airport customs cargo processing and intelligence center.

These examples amply demonstrate that servers and network data drives are not only attractive, but also vulnerable, targets for thieves. In an era where the monetary value of drives and servers continues to decrease, the fact that thieves are willing to risk being arrested while stealing equipment is likely an indication that confidential data is the true objective of their incursions.

Servers can be at risk even inside large, well-managed facilities

Despite standard physical security measures employed at data centers, there are still many opportunities for insiders or skilled thieves to steal important servers and drives, even during normal hours of operation.” For example, when systems are being expanded or modified, there are frequently large numbers of contractor technicians who carry equipment in and out and have the opportunity to remove drives or servers with few questions asked.

Physical security measures are more vulnerable to “social engineering” than online attack protection. As a result, skilled imposters are capable of impersonating fire inspectors, water deliverymen, or service personnel, and can often gain entry into even some of the most restricted facilities. One member of a “tiger team” commissioned to penetrate client data centers explained that it was easy to bypass the front reception area and walk around the side of the building while wearing a hat and shirt from any well-known technology company. There he could blend in with the smokers that frequently congregate outside the side doors during break hours. Then he simply waited until the original smokers went in and others took their place. Because the new group naturally assumed he was a contractor that had already been checked in at the front desk, he was able to then simply walk into the facility, enter the computer rooms and brazenly start removing equipment.

In large data centers it can take a long time before theft is even noticed. Equipment is commonly moved or shut down for various reasons, so administrators might not immediately suspect theft. System logs that would show equipment mysteriously going “offline” might not be examined in a timely or even competent

manner. Often large organizations have entire rooms with old drives or servers awaiting formal decommissioning with little control over access and only a hazy idea of exactly what is stored there. And even if a theft is detected, who knows what was stored on the missing equipment?

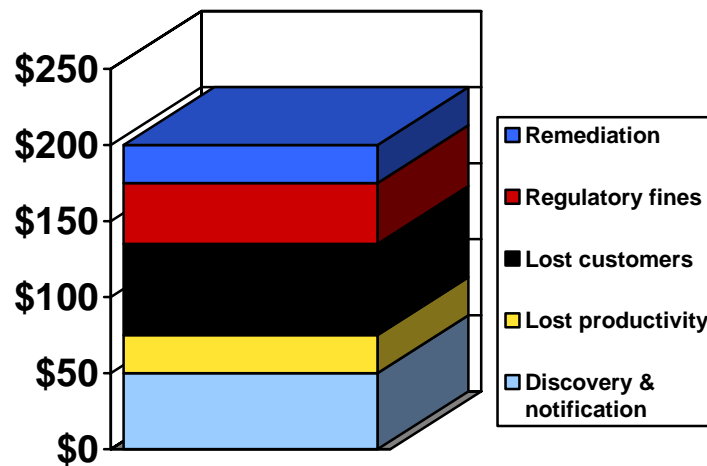
Another potential source of data loss arises when drives with problems are sent outside warranty service depots with the data fully exposed and vulnerable. Frequently drives under warranty cannot be repaired and so a replacement is automatically sent and the original defective drive is forgotten. But what assurances are given that sensitive data on the defective drive has been properly wiped or destroyed?

Consequences

The potential negative consequences of data theft are substantial and growing. Recent studies indicate that the overall costs of forensic research, notification of affected persons or organizations, legal assistance and regulatory penalties range from \$50 and \$300.¹ The Ponemon Institute estimated the average cost per compromised record at \$182 in 2006, up 30% from 2005.² With single machines sometimes containing tens of thousands of records, the risk of substantial financial impact is obvious.

Average Cost per Compromised Record

(Source: Forrester Research)



In addition to class-action litigation, executives of companies that are negligent in protecting regulated data face the very real possibility of criminal charges. The threat of criminal conviction was made part of legislation that governs breaches of private, confidential data specifically to make executives think very carefully about their responsibility to protect such information.

¹ Forrester Research 2007

² Ponemon Institute, 2007

However, the evaporation of trust associated with large-scale data theft may be the biggest loss of all. Since a growing percentage of the market value of companies is related to intangibles such as proprietary technology, partnerships and customer relationships, any event that adversely affects these elements could have dramatic impact. As customers, partners and investors respond to reports of negligence and mismanagement, the market value of the organization is likely to plummet. Unlike a bad financial quarter, a loss of confidence by key stakeholders can cripple organizations for years.

Regulations Governing Confidentiality of Data

In the past five years a growing body of state, Federal and international regulations has dramatically altered the IT security landscape. Government agencies, public companies, and those that deal with personal financial or medical information have all been substantially affected by these regulations. Previously security officers focused mainly on preventing financial loss and maintaining business continuity, but today they must also be able to prove compliance. The common objectives of regulatory requirements are 1) the protection of private, confidential third-party information (such as medical or financial data), and 2) ensuring adherence to procedures that protect the value of public enterprises for investors, particularly those relating to financial and data processing systems.

The effectiveness of encryption in protecting private, sensitive information has been explicitly acknowledged by legal requirements related to data security. All thirty five US states that have passed such legislation have provided an exemption from issuing warning notifications if the data in question was encrypted. As of June 2007 five of the six significant U.S. bills under consideration provide an explicit “safe harbor” for encrypted data. Industry “best practices” standards also emphasize the importance of encrypting data. For example, PCI DSS (Payment Card Industry Data Security Standard) – which establishes a standard for reasonable care in protecting credit card and debit card data by merchants - requires rendering stored cardholder data unreadable. Encryption is the only practical means of meeting that standard.

Summary

Physical security is often mistakenly assumed for servers and drives located in data centers. Additional physical security measures are expensive with many recurring costs, and no assurance of complete effectiveness. Consequently, evidence continues to mount that despite normal precautions, servers and drives can be, and frequently are, stolen even from large, well-managed data centers. Even if the objective is not data theft, the victim must assume the worst case and undertake the same precautionary steps and bear the same costs as if it were. Industry averages suggest it will normally cost close to \$200 per record to respond to theft or loss; and, since many thefts involve tens of thousands of records, the costs can be crippling.

For additional information regarding this study, contact:

John Muir, Managing Partner
jmuir@TrustedStrategies.com
www.TrustedStrategies.com



Stolen Drives and Servers – Don’t Think it Can’t Happen in Your Data Center
Trusted Strategies LLC
www.TrustedStrategies.com

About Trusted Strategies

Trusted Strategies is a research and advisory firm focused exclusively on IT security. We are information security market experts regarding industry trends, technologies, products, and vendors.

Our clients are product vendors who we help with market validation, positioning, competitive analysis, go-to-market strategies, business development, and the creation of marketing and sales tools for their IT security related products. We also assist companies who are buying, selling, or otherwise acquiring IT security technology or firms.

With over 20 years of experience in the field and as successful IT security entrepreneurs ourselves, Trusted Strategies understands the information security industry and how to provide just what our clients need.

Trusted Strategies, LLC
Pleasanton, CA
925 461-1002
www.trustedstrategies.com