ZECURION

Protection from the Inside Out™

Dealing With the Enterprise Data Threat

How Zecurion Protects Corporate Data

Author: Robin Bloor

HURWITZ & ASSOCIATES

Insight to Action

The Realities of Data Theft

The safest way to rob a bank is to use a computer. There are four compelling advantages to this approach:

- You don't risk physical injury or personal harm.
- If you choose your target wisely, the likelihood of getting caught is low.
- If you pull off the heist effectively, you are likely to get away with much more money; 10 to 100 times as much.
- You can attempt multiple robberies at once. It's far more efficient use of your time.

Actually, why just focus on banks? Why not focus on all organizations that have valuable data? And while you're at it, why not enlist the help of an insider, so that when you break through the firewall, you'll have all the information you need to find where the gold is buried.

When you're trying to protect a company's data, you need to protect it from both insiders and outsiders. According to the Info-Tech Research Group, security breaches from insiders outnumber outside breaches by about 3 to 1. According to a Ponemon Institute Survey: Among companies reporting serious data leaks, 69 percent attribute their data security breaches to malicious employee activities or employee error. So the sad truth is that your data needs more protection from insiders than it does from outsiders.

Reports in the press that cover data theft can be misleading; they tend to focus on how the cyberthieves gained entry to a network. Thus the record-setting data heist suffered by TJX in 2007, in which 45 million credit card records were exposed and an unknown number stolen, was depicted as a wireless security problem, because the cyberthieves are assumed to have gained entry to the TJX network by cracking the WEP wireless security protocol.

In fact, no-one is sure exactly how the cyberthieves gained entry, because no wireless security monitoring was being done. That the intruders cracked the known-to-be-unsafe WEP protocol is just the best available theory. TJX simply discovered that unauthorized software had been installed on its systems and that data theft had been happening for quite a while. An insider may or may not have been involved.

This highlights one of the problems of perimeter security. It's necessary, but it doesn't act as a significant barrier to insiders. While high profile data heists seize the headlines, much less is said about casual data theft. Nevertheless, casual data theft appears to be endemic in many organizations.

That is the message of a Ponemon survey published in February of this year, which revealed that 59% of employees with accesss to proprietary data, who leave or are asked to leave an organization, will and do steal data. They steal whatever they believe has value, including customer

304 Park Ave South 11th floor | New York, NY 10010 | Tel: (646) 240-4985 | info@zecurion.com | www.zecurion

data, email lists, contact lists, employee records, financial reports, confidential business documents, software and other intellectual property.

Priorities in IT Security

The conundrum that faces the staff charged with keeping IT secure, is that there is a multitude of different threats. They include:

- Data theft
- Financial fraud
- Malicious damage to computer resources, company web sites or data
- Theft of computer resources (especially laptops)
- Abuse of computer resources (viruses, unauthorized software, etc.)
- Denial of service attacks.

There is a wide variety of IT security products that deal to some degree with one or more of these threats. The security team's problem is where to best spend the money to keep the organization safe. Even when the IT security budget is large, it is not possible to keep an organization completely safe from attack, so managing IT security is actually about managing risk. Consequently, a primary imperative is to prevent very expensive security breaches.

The most costly security incidents involve financial fraud or data theft, particularly the theft of credit card information, which has a particularly high cost - but at least it's a known cost:

Darwin Professional Insurance, an underwriting company provides a specific product, Tech//404 for insuring against data loss and other technology risks. Usefully, it also provides a calculator for calculating the cost of data loss. On a sample of 1,000 credit card records, for example, Darwin's Data Loss Calculator calculates the cost of data loss to be $166 per record.

This is in line with a Forrester Research survey of 28 companies, which found that the cost per record lost for actual data theft was in the range $90 to $305.

The major costs stem from:

- The cost of the internal investigation that follows any data theft incident.
- The cost of crisis management, particularly notifying affected customers.
- The costs of regulatory compliance, including state and federal fines and fees.

There is also a reputational cost which may exceed all of these costs.

304 Park Ave South 11th floor | New York, NY 10010 | Tel: (646) 240-4985 | info@zecurion.com | www.zecurion

Encryption as a Shield

The table below displays data from the 2008 CSI/FBI survey on the use of IT security products and technologies. It illustrates a paradox in IT security. While all of the technologies listed are important, it is surprising, perhaps even disturbing, that data encryption is not much higher on the list. This is especially the case given that there is no record of properly deployed strong encryption technologies ever being broken, even by brute force cracking.

If data is encrypted, so long as it remains encrypted it is useless to anyone who steals it. The paradox is explained by the fact that historically, although encryption technology has been highly effective, it has also been an inconvenience. Particularly, encryption has presented the following problems:

- Encryption/decryption presents a processing overhead.
- The management of encryption keys can be difficult, either because it creates vulnerabilities or because it imposes inconvenient procedures. If an encryption key is lost then the encrypted data is irretrievable. The data might as well have been deleted.
- The direct use of encryption technology by applications can require programming or an inconvenient configuration effort.
- Once decrypted, the data is vulnerable. Consequently encryption/decryption needs to be centrally and precisely managed.

Technology	Use
Anti-virus Software	97%
Firewalls	94%
Virtual Private Networks (VPNs)	85%
Communications Encryption	71%
Intrusion Detection Systems (IDSs)	69%
Vulnerability & Patch Management	65%
Data Encryption of Files & Databases	53%

Adaptive Multithreaded Encryption from Zecurion

Zecurion is a company that has built encryption technology to solve the encryption problems we have described. A testimony to its success is that fact that it currently has about 5,000 corporate customers, mainly in Europe. The reasons for its success are that it is scalable, flexible, unobtrusive and very easy to use.

304 Park Ave South 11th floor | New York, NY 10010 | Tel: (646) 240-4985 | info@zecurion.com | www.zecurion

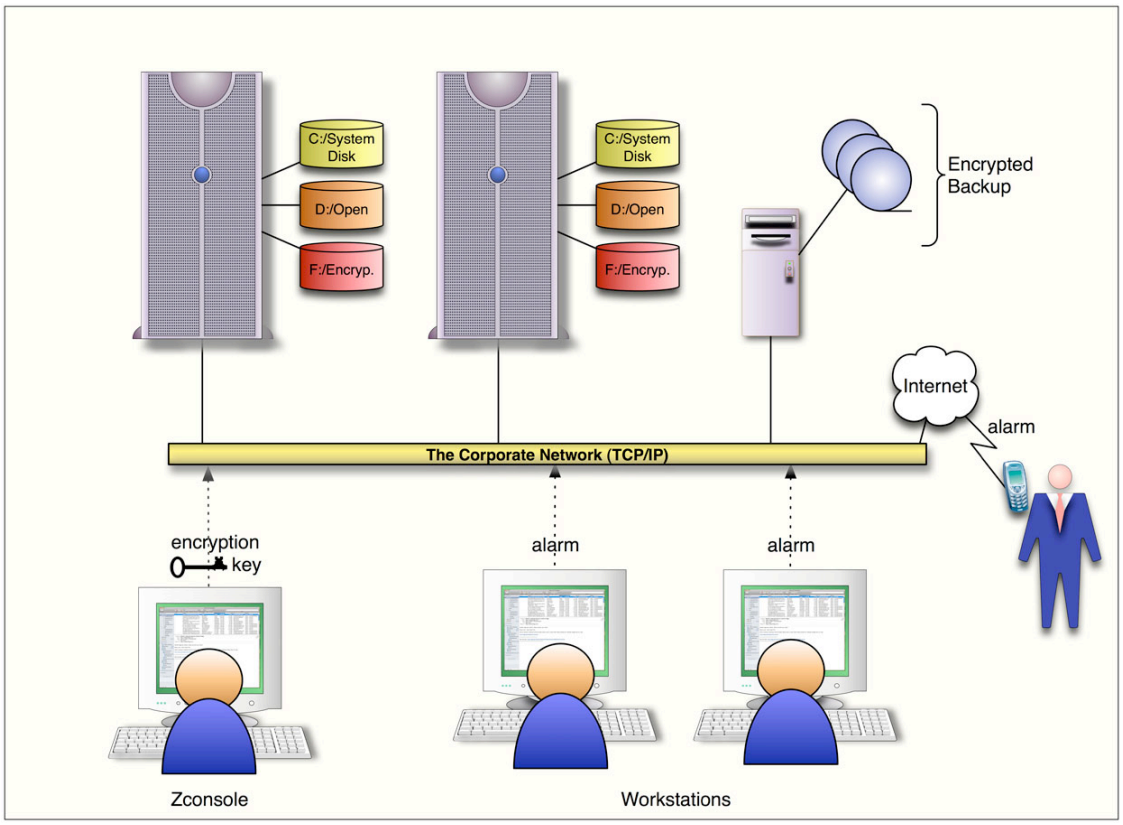

Figure 2. Zecurion Zserver Architecture

It is possible to map access to data on a user-by-user basis or by user groups or roles, so that some encrypted data is available to some users, while others do not even know the data is there.

The first point to note about Zecurion's Zserver Suite is that it is software that inserts itself painlessly between the application (or the user) and the storage devices. As far as the user is concerned the encryption process is invisible and becomes visible only if the user tries to find a way to access raw data on the disk. The files that are encrypted are not even visible to the user. It is possible to map access to data on a user-by-user basis or by user groups or roles, so that some encrypted data is available to some users, while others do not even know the data is there.

As illustrated in Figure 2, Zserver creates a separate partition on the storage device, which can be thought of as a separate logical drive. It works with any device, including RAID arrays and SANs. Not only is the data encrypted, but the volume system data is also encrypted. You could steal the physical disk and it would be impossible to get at the data without the encryption key.

Encryption can be applied to or removed from data at any point in time, using the Zconsole. If for any reason there is a need to remove encryption completely then it can be switched off from the Zconsole. In an emergency it is possible to lock down all data by sending an alarm from any device, including devices connected through the Internet. This removes the encryption key from memory

304 Park Ave South 11th floor | New York, NY 10010 | Tel: (646) 240-4985 | info@zecurion.com | www.zecurion

on a specific computer, making all its encrypted data inaccessible. Such an action would be taken if it was discovered that someone was in the process of trying to steal data using an authorized application. The data can be made available again simply by re-entering the encryption key.

A second product, Zserver Backup, is used for backups, using the same AES 256-bit encryption. This component is compatible with every kind of backup device; tape, DVD, WORM Disk etc. It can be used with tape libraries and commonly used backup software; BrightStor ARCserve, Symantec Backup Exec, etc.

Adaptive Multi-threaded Encryption Architecture

Zecurion's encryption technology has an adaptive multithreaded architecture. This means is that the encryption software splits encryption and decryption activity into several concurrent tracks assigning work to different cpus, so that the work of encrypting and decrypting data is distributed and does not present an unacceptable performance overhead.

The software is designed to make use of all processors available to it, so it can be scaled to fit any workload. This feature effectively lays to rest the performance concern of using encryption technology.

Encryption Key Management

Perhaps the most troublesome element of encryption is managing the encryption keys. This is the place where most encryption technology falls down. Unbreakable encryption schemes have been available for a long time. Whenever brute-force approaches to cracking the encryption using very large amounts of computer power become feasible, it is only necessary to increase the encryption "span" from 64 bit to 128 bit or from 128 bit to 256 bit and so on. The main vulnerability is in the encryption key itself. Once the performance problem is solved, the main difficulty with encryption systems is in the secure management of the keys.

There are two possibilities that need to be catered for:

1. Key loss
2. Dishonest key holders

Encryption keys might be lost. Zserver, for example, holds encryption keys on smart cards or USB tokens (the Zserver encryption key is not something you'd want to try to memorize). So what happens if a smartcard holding the encryption key gets lost?

Well, if it is the only copy of the key, then you are in trouble, because now you can no longer get at any data. The impact would depend on what situation your systems were in, but it would probably be catastrophic.

So it would be better to have several copies of the key (on a smartcard, or whatever) keeping some in reserve in case one is lost. But if one gets lost, maybe it was stolen, or even if it was not, it might fall into the hands of someone with criminal intentions. So you would have to be very careful with any copies of the key. If a copy of the key is lost, the key has to be changed. That would be inconvenient, and it would probably be expensive.

When it comes to the possibility of dishonest key holders, the situation gets even worse. Practically it may not be possible to provide the key to just one person - people cannot be on-call 24 x 7 forever. But as soon as you trust more than one person with the key, you increase the possibility of having a dishonest key holder. You need only one dishonest key holder to ruin the whole encryption scheme.

Zecurion has overcome the problem of key management in a simple but ingenious way. The Zserver encryption keys can be split into multiple components. For example, you might split the key in 3 parts and give each part to 3 different people, but only two of the 3 parts would be necessary to restore the original key. Then if a key is lost or destroyed there is no vulnerability. Neither is there any need for 24 x 7 availability of key holders. You could even change the key holders on a regular basis.

In Conclusion

Ultimately, encryption is a necessary defense for securing valuable data because it dramatically narrows the window of unauthorized access to data. The simple fact is that encrypted data is much more difficult to steal.

The popularity of Zserver is clearly no accident. It has laid to rest several difficult problems that have plagued encryption technology for years and which explain why encryption technology is not as widely used as it should be.

The bottom line is this:

- Zserver is unobtrusive and flexible. It can be deployed in a manner that is not obstructive to users - except those who seek unauthorized access to data.
- Zserver's multithreaded encryption architecture eliminates the performance degradation that has traditionally been associated with encryption. The solution is scalable.
- The solution is software. It does not require specific hardware (such as an encryption chip) and hence it can be deployed anywhere in a network.

304 Park Ave South 11th floor | New York, NY 10010 | Tel: (646) 240-4985 | info@zecurion.com | www.zecurion

- The key management problem is solved and the solution is highly flexible allowing an encryption key to be divided up in multiple ways that eliminate the danger from dishonest key holders and the danger of inadvertent key loss.

Given this set of capabilities, it suddenly becomes possible to deploy encryption in a strategic manner throughout an organization, protecting data from external intruders, dishonest internal staff and accidental exposure through user error. As such, in our view, with Zecurion, encryption is now enterprise ready.

About Hurwitz & Associates

Hurwitz & Associates is a consulting, research and analyst firm that focuses on the customer benefits derived when advanced and emerging software technologies are used to solve business problems. The firm's research concentrates on understanding the business value of software technologies, such as Service Oriented Architecture and Web services, and how they are successfully implemented within highly distributed computing environments. Additional information on Hurwitz & Associates can be found at www.hurwitz.com.

About Zecurion

Zecurion is a leading global provider of security protection of corporate information from internal threats, emphasizing reliable and transparent backup encryption, server storage security, email security as well as control of peripheral devices in corporate networks with clear, easy-to-use administrative interfaces and tools. Zecurion's unique forensic capabilities are unmatched, providing an additional layer of risk management through the shadowing and storage of communications transactions for future auditing.

Zecurion's solutions are successfully protecting the internal assets and intellectual property for more than 7,000 companies worldwide. Zgate, Zlock, Zserver, and Zdiscovery have been recognized for technology and security protection. Zecurion is led by an executive team experienced in developing security software and deployment across the enterprise. With over a decade of experience in developing encryption-based security solutions, Zecurion allows IT departments to efficiently protect corporate information from internal threats, as well as from loss or theft of backup storage media.

As organizations realize the operational and financial benefits of cloud computing and transition data storage from internal resources to cloud-based data storage services, Zecurion provides an effective, intuitive, and cost-effective solution for encrypting and protecting sensitive data no matter where it resides.

304 Park Ave South 11th floor | New York, NY 10010 | Tel: (646) 240-4985 | info@zecurion.com | www.zecurion