



## The Missing Link in your system security?

Paul Howard

paul@bosanova.net



*A Tradition of Excellence*



- View of security in general
- Storage security
- Backup and Archive
- Transporting tapes
- Record losses on tape
- Ways to protect against data loss on tape
- Conclusions



### **Security – Majority focus is on Network Security**

Physical Access controls with only those people required given access to the computer room and a log kept of entry and exit.

- Access rights to data controlled by password, biometrics, and time periods etc.
- Firewalls used to ensure only those with the correct credentials to gain access.
- Intrusion prevention & detection software.
- Anti-virus and anti-spyware software to protect against Spyware, Adware, Viruses, Trojans, Worms, Key loggers and other threats.



***Conventional Security thinking.***



## **Security – Majority focus is on Network Security**

This sometimes results in the “Fortress mentality” – Think everything is secure and safe!



***A Tradition of Excellence***



## **Look at Storage Security**

The security of the "data at rest".

Any data on magnetic or optical media such as discs, CDs, tapes etc.



## Look at Storage Security

Internal security such as disc in a RAID is a possible concern.

If it is an internal theft it would be quite obvious if drives from a RAID set are removed.



## Look at Storage Security

Loss of the complete computer system is also possible but Physical Security should stop this.

This is less likely to happen but needs to be addressed as part of the overall security plan.



## Archive and Backup

- **Archive** is long term storage of data on a removable media normally not expected to be required often or at all. *Examples – Old insurance policy documents that legislation requires to be kept for a number of years but that are no longer valid.*
- **Backup** is a regular copy onto (normally) removable media of live data on the system which is made in case the live system data is lost, corrupted or not available for any reason.



- Basics
- Take a regular backup of the data to a removable media, normally this is tape
- Make sure this covers all the required information to ensure the system can be restored in the event of a disaster.
- Test the system and file restores on a regular basis.



- Basics
- Make sure the tapes are removed from the site to somewhere they are easily accessed if you do have the need to invoke your DR policy



Now you have everything safely backup up onto tape and taken to a safe off-site facility consider what is on those tapes.

# **Your business!**



## *Transporting tapes*



You will be regularly shipping a number of tapes to either your own DR site, a shared DR site or a “secure” off site store.

This can be via your own company vehicles, specialist data courier or regular courier.

This is the weakest link in the chain!



# Transporting tapes



All of these companies have been involved in the loss on tapes



*A Tradition of Excellence*



## *Transporting tapes*



Your insurance policy will normally not cover the impact of the loss of data on tapes in transit.

The courier company will cover you for the loss of the physical media, not the data contained on it.

People handling the tapes often just see them as a low value item.



# Record losses on tape



Date	Company	Reason	Records Lost
Jan 2007	Independent Living Funds UK	Stolen tapes	19,000
Jan 2007	U.S. Internal Revenue Service	Lost /stolen	Unknown (26 tapes)
Jan 2007	Anthem Blue Cross Blue Shield Virginia	Stolen tapes	50,000
Jan 2007	Canadian Imperial Bank of Commerce	Lost tapes	57,000
Feb 2007	Johns Hopkins University & Hospital Baltimore	Lost /stolen	135,000
March 2007	Dai Nippon (Japan)	Stolen	9,000,000
April 2007	Florists' Mutual Insurance Co. (Hortica)	Lost /stolen	Unknown
May 2007	J P Morgan	Lost / Stolen	47,000
May 2007	IBM	Lost	Unknown
June 2007	Ohio State Workers	Stolen	500,000
July 2007	Gils Scouts Mile High Denver	Stolen	Unknown
September 2007	University of Michigan, Nursing School	Stolen	8,585
September 2007	State of Connecticut	Stolen	58
October 2007	West Virginia State	Lost	200,000
October 2007	Hartford Financial Services Group Inc.	Lost / Stolen	237,000
<b>Total lost in 2007</b>	<b>10,253,643</b>		



A Tradition of Excellence



# *Record losses on tape*



Why have these losses been made public?

## ***Legislation***



## ***Record losses on tape***



Most states have either passed laws, or are in the process of doing so, that require any data loss of personal records is reported.

Started with California's Senate Bill 1386 which essentially, *requires an agency, person or business that conducts business in California and owns or licenses computerized 'personal information' to disclose any breach of security (to any resident whose unencrypted data is believed to have been disclosed).*



# Record losses on tape



## **Requirement 3: Protect stored cardholder data**

*Encryption is a critical component of cardholder data protection. If an intruder circumvents other network security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person.*

3.4 Render Primary Account Number, at minimum, unreadable anywhere it is stored (including data on portable digital media, backup media, in logs, and data received from or stored by wireless networks).

**Full details at [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)**



# *Record losses on tape*



- S-OX - Sarbanes Oxley Act of 2002
- HIPPA - Health Insurance Portability and Accountability Act of 1996
- GLBA - Gramm-Leach Bliley Act
- Basel II - International Convergence of Capital Measurement and Capital Standards
- FISMA - Federal Information Security Management Act of 2002
- ISO/IEC - International Security Standard for Information  
27002:2005



# Record losses on tape



## Gartner

*"From lost laptops to misplaced backup tapes to accidental e-mails filled with sensitive information, we seem to be in the midst of a data loss epidemic, with tens of millions of individuals receiving 'data loss' notification letters this year," said Rich Mogull, research vice president for Gartner.*



The Ponemon Institute research firm reported that data breaches cost companies an average of **\$182 per compromised record** in legal fees and other expenses.



## *Ways to protect against data loss on tape*



Don't remove tapes from the secure area.

Increase physical security when moving the tapes.

Encrypt the data so that they cannot be read by other people.



## *Ways to protect against data loss on tape*



As made clear in the PCI regulations making these backup tapes unreadable by other people by using encryption is the way to proceed.

Losing an encrypted tape does not need to be reported.

Like most things in life there are many ways to achieve this and many decisions to be made.

Not all are obvious!



Decision one:

Encrypt everything or just the "sensitive data"?

You can minimise the processing required by just doing selective data.

The issue is how to decide what is sensitive and how to monitor this selection on an ongoing basis. Rules set up to select this might not cover all things in the future.

It is possible to do this but needs a great deal of planning, management and control. *For most users this is not a practical solution.*



## Decision Two: Software or Hardware?

Software appears to cost less but the processing overhead this can add often makes this non practical.

Using software requires you either have a backup package that has this option or you change to one that does.

Software will need to have the keys reside on the server, however well protected this is always a security concern.

With software the only thing different between your system and another users will be the key.



## Decision Two: Software or Hardware?

Using software you will need to have the software up and running with the encryption configured before starting a restore.

Software can be open to attack by viruses and Trojan horses.

When the system is upgraded there may be issues getting the software upgraded.

If you need to convert your existing tapes this will be time consuming and use system resources heavily if even possible.

Software might be suitable but these and other considerations need to be taken into account.



## Decision Two: Software or Hardware?

Hardware allows for all the processing to be done without using any extra system processing.

Hardware can work with any system hardware and backup software. No need to change software or procedures.

A hardware solution can securely keep the keys internally.

With hardware it is possible to have unique hardware keys so that even someone with your users keys cannot read the tapes on another companies similar hardware.



## Decision Two: Software or Hardware?

Using a hardware solution you can do a complete system restore without needing to configure the system for encryption first.

A hardware solution makes off-line conversion of the existing tapes possible.



## Decision Three: In line or built in?

- An in line solution allows you to utilise existing media
  - Tape drives with built in encryption normally require new media.
- Tape drives require external key management.
  - In line appliances do not always have this need.
- Not all systems support the new tape formats.



Hardware offers the simplest and most flexible solution to meet compliance across all platforms.

In line solutions offer the least disruptive method of implementation for small and mid size systems.

In line solutions are available on all hardware systems types, operating systems and backup software.



***Our Solution!***



***A Tradition of Excellence***



***Our Solution!***



***A Tradition of Excellence***



## ***Our Solution!***



- Q3 – An in-line hardware encryption appliance.
- Field proven 3<sup>rd</sup> generation design.
- Range of interfaces to suit different environments.
- Interchangeable across the range.
- Host, software and drive agnostic.



## ***Our Solution!***



- Simple to use
- Simple to integrate
- Simple to understand
- No prescriptive key management
- Works on all platforms
- No new media required
- No changes to system or basic procedures
- Competitive pricing



**Questions?**



***A Tradition of Excellence***

