

# WHITEPAPER

6 Common Misconceptions about the Protection of Backup Tapes

---

---



Every time there is a reported incident of a company losing backup tapes, the standard response given by the press office seems to go along the lines of “Because our system is proprietary you can’t read data from the tapes without very expensive hardware and software technology, and a similar host environment.” This essentially says to the affected customers whose data was on the tapes that they need not worry about it.

What’s the reality behind this statement? It portrays the company as taking all steps reasonably possible to protect the sensitive information contained on the “lost media.” It also has the hand wringing affect of “what else could we have been expected to do.” But is this a reasonable response?

This article demonstrates that these statements are unrealistic and unacceptable and show a complete lack of understanding of the security implications. Evaluated below are the 6 common misconceptions about the protection of backup tapes:

1. Data on a backup tape is too difficult to recover.
2. Old backup data is useless.
3. Backup data written with certain mainframe or midrange systems cannot be read without the appropriate expensive equipment.
4. Tapes can be password protected.
5. If the backup tape has been found, it means that your compromised data is no longer at risk.
6. Companies need not worry about thieves stealing backup tapes because they don’t have the means to recover such information.

### **The Fantasy**

One only has to look in the press to see numerous examples these common misconceptions about backup tapes.

---

**BOSaNOVA, Inc.**

**Phone:** 866-865-5250 **Email:** info@theq3.com **Web:** www.theq3.com

A news item on the BBC in April 2008 reported that *“the details of 27,000 customers and 7,000 employees were stolen from Boots Dental Plan on 3 April.”* The report goes on to say *“The information from Boots Dental Plan included customer bank account details, but officials claimed it was “highly unlikely” these could be accessed.”*

The implication that this is not a problem was given by stating.

*“The data is described as “technically complicated” and only accessible with specialist IT equipment and software.”*

The data tapes were stolen from the vehicle of a data security company while on a scheduled delivery to a Medisure office.

### The cost of a data breach

A recent Ponemon Institute survey of 9,000 people found that 12% of respondents had been notified of a data breach or loss by a company with which they did business. Of those affected, 20% said they immediately stopped doing business with the companies that couldn't keep their data secure. Can you afford to lose 20% of your customers?

For years certain system users were convinced that their information was secured by the obscurity of the system and maybe that is what encourages this attitude from the people generating these press releases. The supposition that anyone finding the tapes needs the same systems, and of course still needs to overcome the passwords that protect access to files, allows many a CIO to sleep soundly at night, but the reality is far from this.

Another reason why people still maintain it will be difficult for someone else to restore their lost data may be because they perceive it is difficult enough for them to do it so for someone else it would be next to impossible. The reason for some of this view is that too many companies do not invest in the staff, time or equipment to fully test their DR capabilities on a regular basis. What happens is that they only try to restore data when it is needed in an emergency so use untested procedures that result in either failures or a difficult and long process.

**BOSaNOVA, Inc.**

**Phone:** 866-865-5250 **Email:** info@theq3.com **Web:** www.theq3.com

### The Reality

If you have a backup tape from someone's system XYZ, and you restore it on your system XYZ, you are of course the administrator on your system and can give user rights and access data restored to it. This means you can access all that data quite easily, unless there are some very specific extra precautions being taken on the original system. On most systems full access to all the data is straightforward and simple. This is of course if you have a similar system. If you don't there are ways to access the information contained on these tapes even if you have no indication as to what system type or the operating system they were written on.

### What's on the Tape?

It is worth understanding just what data is contained on these tapes. Usually when a loss is admitted the company evaluates the number of customer records on the tape and whether it contains social security numbers, credit card information or similar clearly sensitive and valuable data.

Clearly this is very important information but for a moment let us consider what else that could be on a tape and what impact the disclosure or loss of that could have. It is likely that the records will contain notes about a particular customer's dealing with the business that has lost the tapes. This could contain information that would be potentially damaging to the person or business that the record refers to. It might for instance show bad debts or poor payments or other information that could be detrimental to that person or business.

The tapes are also likely to contain all the HR details of the staff of the company. Again this can be damaging but in this case is more of a worry to the company that has lost the tapes as staff and shareholders might find out about salaries paid and perks given to senior management. Industrial unrest could soon follow and the damage to the business could be substantial.

It is often presumed that "old data" is useless. It may be true that doing a system restore from data more than a week old might not be any use to the company

---

**BOSaNOVA, Inc.**

**Phone:** 866-865-5250 **Email:** [info@theq3.com](mailto:info@theq3.com) **Web:** [www.theq3.com](http://www.theq3.com)

because much can have changed within even a week. If however we look at the use of that information for fraudulent purposes then the picture is very different. What the thieves need are the background details allowing them to transact purchases, open accounts and similar processes. The “old data” has the SNN, address, bank account numbers, home address and other very useful information that is just what the thief will use to steal someone’s identity or transact fraudulent purchases.

### So How Can It Be Read?

For years the IBM AS/400 (iSeries) community lived with the view that their system was a secure and safe system and looked out at all the security issues reported on the Windows servers with little disguised disdain. They failed to understand even their backup tapes, written in EBCDIC (Expanded Binary Coded Decimal Interchange Code) can be easily displayed on a simple PC with a straightforward tape dump routine. It is quite straightforward to dump these details and start to use the information gained on that same simple PC. Identity theft using this method can result in millions of people being affected just by the loss of one tape.

Another reason given in the past was that the thief or person finding a tape would not have the right tape technology to be able to read the tape as this was restricted to mainframe and midrange systems only. This is no longer true with very high capacity drives being made available at a low cost on the likes of e-bay and similar auction sites. Major companies see their large tape silos as very high price tag items but overlook that the drives contained in them are very often available to the world as low cost desktop devices. These units are easy to acquire at a low cost and may not transfer the data at the high transfer rates as those found in the large tape silos, but the tape formats are the same and therefore can be read easily.

When evaluating the vulnerability of the information on tape a simple method to look at is one of the many programs available that can “dump” the content

to the screen and allow reading of the information direct from the tape regardless of the system and software used to generate it. Using a free download of such a program and a drive bought on e-bay, Bob Cozzi of iSeries TV showed how straightforward it was to display the data on an iSeries tape. Bob used TapeWise ([www.tapewise.com](http://www.tapewise.com)) software and a DELL LTO drive bought from Ebay and his full video can be seen at <http://www.theq3.com/video.php>

### **Password - What Password?**

Another reason given as to why we don't need to worry that a company has negligently allowed our personal data to escape is because it is password protected! This again leads us to believe that the people whom have been entrusted with our vital personal information just don't understand security at all. If they believe that you can password protect a tape then what other security holes do they have in their system?

The other statement we often see is, "We have no reason to believe the missing data has been used." The idea that this data must be used straight away to be of any use also shows a lack of understanding as to how this type of information gets used. The thief only needs to store the data and wait for the users to start to relax, maybe for the banks and credit card companies to minimize the monitoring of those accounts, and then they start to use the information gathered. SSN's, the user's address, date of birth, place of birth and other useful information is not likely to change over an 18 month period so the thieves can afford to wait before making use of that data.

A tape can be copied quickly and easily and there's no way to see or monitor if this has occurred. Once copied the thief has all the time he needs to discover the format of the saved data and then restore what he needs. The simple way may just be to do a easy "dump" of the data on the tape and then use that.

### **Copied Tapes**

Sometimes we hear that everything is OK as the missing tapes have been found but this can be an even more worrying state. Where were the tapes, who

---

**BOSaNOVA, Inc.**

**Phone:** 866-865-5250 **Email:** [info@theq3.com](mailto:info@theq3.com) **Web:** [www.theq3.com](http://www.theq3.com)

had access to them and could they have been copied while they were missing? In this case the compromised account may not be flagged up for special monitoring of unusual activity so can be more at risk than those tapes that are deemed missing.

According to the Identity Theft Resource Center, in 2007 there were over 446 security breaches affecting nearly 120 million individuals.

Lost or stolen backup tapes contributed to a large number of these breaches.

### **Tapes are Now Being Reported as Stolen**

A worrying trend that is becoming apparent is the increasing number of tapes that are being flagged as having been stolen. This might be simply because the reporting process has been improved, but may indicate that as security on the electronic access to systems has improved, thieves have started looking at simpler ways to get the information they trade. High capacity tapes now can easily contain over one million complex records so their value is more significant to the thief. A recent report in the Washington post gave a figure of \$14 per record as the value of the stolen information. As single tape with say just 100,000 records could be therefore worth \$1.4M to a thief.

A disturbing report by John Dunn on Techworld shows details on a website supermarket for stolen card data:

The 'SellCVV2' website was found to be trading the card numbers and other data in a number of sophisticated ways. Criminals visiting the site would be able to earn discounts based on volume bought and choose from a range of tiers, starting at the least valuable Classic Visa or MasterCard - those with the lowest credit limits - through more valuable Gold, Platinum, and Corporate levels.

According to Finjan, prices ranged from \$38 (£20) for small volumes of premium card numbers, down to \$10 (£5) for the

**BOSaNOVA, Inc.**

**Phone:** 866-865-5250 **Email:** info@theq3.com **Web:** www.theq3.com

equivalent low-limit cards in chunks of 100 at a time. Criminals worried about being stung themselves by non-working cards were being offered 'guarantees' as well as trial data sets.

Sensible people will be considering that if these tapes contain such valuable information, "why are they being transported around and getting lost and stolen all the time?" Tape backup is still the most common way for companies to ensure that in the event of some catastrophe they are easily able to get their business back up and running. Typically tapes are taken offsite for disaster recovery reasons. Most companies employ a professional company to transport their tapes but even these companies lose the tapes (they recommend that companies encrypt their backup tapes.) Now that thieves are realizing the value of the tapes these types of courier companies are more likely to be targeted.

Encryption for tape is simple, has been available for more than ten years, is available to be utilized on all systems and drive types and needs no software, drivers, or agents to be added to the system, so why aren't all companies that hold private and confidential data encrypting their backup tapes?

### **Responsibility to Protect**

In 2005 the United Nations World Summit accepted the concept of "the responsibility to protect" and heads of state and government from 150 countries unanimously signed up to this. What this said in basic terms was that sovereign states have an explicit responsibility to protect their own people from war crimes, genocide, ethnic cleansing and crimes against humanity but if they failed in that responsibility – then the wider international community have the responsibility to take whatever action that is necessary. A lecture on this subject given by Gareth Evans, President of the International Crisis Group, in April 2008 was titled "The Responsibility to Protect: An Idea Whose Time Has Come .. And Gone?". We feel that for information security the "Responsibility to Protect" the time has now come.

---

**BOSaNOVA, Inc.**

**Phone:** 866-865-5250 **Email:** info@theq3.com **Web:** www.theq3.com

Companies need to understand their “Responsibilities to Protect” our data and realize that if they fail to do so then the authorities will have the requirement to take action to enforce this. Laws and regulations are being enacted across the world because companies are not taking the correct actions on their own initiative. We need to get a corporate sign-up to the “Responsibility to Protect” or the whole IT industry will find itself heavily regulated in ways that will start to seriously impact the business.

### **Impact of Lost Information**

We see the major financial institutions making it clear that identity theft is on the increase and that we, the users of credit cards, internet banking, etc. are the ones who need to take care of our information. They highlight phishing attacks and simple carelessness of how people record their information on home PCs and PDA as the weak link. It is clear however that the risk can actually be at these very institutions that are trying to tell us we need to be careful. Clearly the attacks on the major companies are likely to be more worthwhile than trying to target individuals home PC's but wherever the leak occurs the damage can be catastrophic to the affected person. Once you lose your credit rating it is hard to recover it even if you were completely blameless.

### **What is the value of your personal data?**

You think your personal information is priceless. But everything has a price, even your stolen bank account information.

McAfee Avert Labs discovered a price list that criminals use to buy and sell credit card numbers, bank account log-ins, and other consumer data that have been filched from unsuspecting Web surfers.

“Last Friday morning in France, my investigations lead me to visit a site proposing top-quality data for a higher price than usual,” writes Francois Paget of McAfee. “But when we look at this data we understand that as everywhere, you have to pay for quality.”

---

**BOSaNOVA, Inc.**

**Phone:** 866-865-5250 **Email:** [info@theq3.com](mailto:info@theq3.com) **Web:** [www.theq3.com](http://www.theq3.com)

## 6 Common Misconceptions about the Protection of Backup Tapes

---

For example, a Washington Mutual Bank account in the U.S. with an available balance of \$14,400 is priced at 600 euros (\$924), while a Citibank UK account with an available balance of 10,044 pounds is priced at 850 euros (\$1,310).

There's even a guarantee that if the buyer is unable to log into the account within 24 hours, maybe because the owner of the data cancelled the account, the buyer can get a replacement stolen account to use.

### **Encryption Solution from BOSaNOVA**

BOSaNOVA offers two storage security solutions for financial institutions looking to protect their data at rest. The Q<sup>3</sup> is a stand-alone storage encryption appliance that's easy to use and has little effect of current backup procedures. The Q<sup>3</sup>i is a tape drive with built-in PCI compliant encryption. For more details, visit [www.theq3.com](http://www.theq3.com) or contact BOSaNOVA at 866-865-5250 or email [info@theq3.com](mailto:info@theq3.com).

BOSaNOVA  
2012 W. Lone Cactus Dr.  
Phoenix, AZ 85027

Phone: 866-865-5250  
Fax: 623-516-8697

Email: [info@theq3.com](mailto:info@theq3.com)  
Web: [www.theq3.com](http://www.theq3.com)

---

**BOSaNOVA, Inc.**

**Phone:** 866-865-5250 **Email:** [info@theq3.com](mailto:info@theq3.com) **Web:** [www.theq3.com](http://www.theq3.com)