



# *Best Practices for securing your backup data*

A whitepaper from DISUK Limited

By Paul Howard

## Best Practices for Securing Your Backup Data

---

### **Data Protection Challenge**

Encryption, the process of scrambling information to make it unreadable to the average human dates back to the Romans. Formerly reserved for high level government agencies, the 1970s saw a shift in encryption practices, making encryption more readily available for new applications in e-commerce, telecommunications and finance.

Now, with security breaches commonplace in the daily news, the need for encryption has become so necessary that various agencies have seen a need to step in and impose regulations. But first, let's ask the obvious question: Why is it even necessary to encrypt backup data, and why is the topic receiving so much attention? The reason is security. Data stored in clear-text is open to attack by everyone from service providers to partners to evil insiders.

Once you know how, it isn't that hard to do. Common firewall technologies, VPN's, and IPS systems do protect the perimeter of the network and offer some security. But they do not change the fact that the data is still stored in clear-text, leaving it ripe for the taking.

### **Off-Site Storage = Defenceless Data**

Although regulatory compliance was originally implemented to assure standardized corporate financial reporting and auditing practices, IT organizations are beginning to address its widespread implications, realizing that, since IT supports the infrastructure of business, the reach and effect of these laws impacts their procedures and processes. Although several sources for guidance are available, there is currently no specific set of guidelines for compliance within the IT industry. However, one area of compliance that remains high-risk is that of data encryption. For the most part, data transported to off-site storage is not secured and tracked, leaving tapes defenceless against theft, alteration or unauthorized viewing. Encryption of backup tapes is the only way to ensure data at rest is safe.

The California Security Breach Information Act (aka CA SB 1386) of 2003 is an excellent example of the direction being taken with these new regulations. Created to address data security breaches in California, this cutting-edge law enforces a rule stating California residents must be notified any time their "personal information" is compromised. This applies to a last name with first name or first initial, and other identifying information such as a social security number, driver's license number or California ID card.

## Best Practices for Securing Your Backup Data

---

It also extends to bank account numbers, credit and debit card numbers, and access passwords or security codes. With the population of California representing approximately 12% of the United States population, it is unlikely a security breach could occur without containing some personal information from a California resident. Of course, this law imposes strict requirements for public disclosure, the main reason for the increase in reported security breaches across the country. In reality, it's better reporting, not a sudden influx of incidences, that have caused this increase. The difference today is that those responsible will have to pay for their mistakes. So how devastating might it be if an IT Manager fails to properly encrypt company data?

Hang on to your hard drives because, depending on the regulation that has been broken, the sentences range from suspension to 10 years in prison, with fines from \$100 to \$1,000,000.

With new regulations raising the bar on regulatory compliance, what was once considered an adequate backup process may become an adequate reason to end up behind bars.

### **How to Begin? With An Honest Risk Assessment**

Therefore, concern is steadily growing over an individual company's current and potential liability. To honestly assess your risk, several key questions must be answered immediately.

- What process controls are currently in place for database management?
- Can you describe the monitoring and reporting currently being used?
- When was the last time you ran tests on your process controls to identify "leaks" and make suggestions for improvements?
- Are you willing to fully understand and accept your own responsibility for managing the internal controls of the databases you manage?

Honest answers to these questions allow you to define what your most critical data is and how best to encrypt that data while at rest. To do this requires an in-depth review of current encryption policies, including assessing methods, key lengths and key management. Only after this thorough process will your company be in the position to address these high-risk areas with proper encryption.

## Best Practices for Securing Your Backup Data

---

### **What's Stopping You from Encrypting NOW?**

Historically, data backup is a task fraught with procrastination. The complexity of the process is time consuming and costly, incurring unacceptable downtime and slowing of networks. VPN, firewalls and other security measures are widely implemented to protect data, however these are not nearly effective enough to provide the security that guarantees the safety of stored confidential records. In times past, corporations were concerned only with disaster scenarios; what if something happened to their on-site backup tapes?

The answer was to transport backup tapes off-site for protection. However, as corporations grew increasingly computer and Internet savvy, the risk of employee theft, data lost or stolen during transport, environmental damage and theft of discarded tapes grew. Each of these threats brought increased security measures.

However, the biggest threat to confidential information today comes not from the outside, but from the inside. And, with over one billion Internet users, Internet hacking has quickly become the most efficient method of stealing data. In most settings, it is the database administrator (DBA) who has oversight of all access to corporate data, and who performs regularly scheduled tasks like importing and exporting data, creation of various reports, and maintaining the performance and stable environment of the database.

Under the new compliance regulations, DBA's find themselves charged with a high level of duties for which they often feel they do not have the most effective arsenal of tools.

### **Everyone is a Risk, From CEOs to Programmers**

For IT managers, it is vitally important to understand the kinds of processes your department has implemented that will prevent unauthorized access to databases, which could lead to altering of confidential database information, as well as accidentally or deliberately destroying precious data. Logic would tell us that the risk personally and to company information and customer privacy is high enough to immediately begin a solid plan of data encryption.

While changes in attitude about data encryption have been slow in coming, many CEOs are realizing the impact that security breaches can have on their bottom lines. Concerned CEOs searching for ways to minimize risk are taking a longer and harder look at cost-effective ways to make data security a priority.

## Best Practices for Securing Your Backup Data

---

The cost of information security and protection is fast becoming the number concern across corporate America, as the risks to confidential corporate data and personal safety increase.

Government regulations, including more stringent control and audit requirements, are designed to protect consumer data and confidential information, making it clear in no uncertain terms the penalties and fines one could face for failing to meet these requirements.

No corporation is immune to the risks involved in failing to encrypt backup data, not even companies responsible for storing the very data we strive to protect. A story released in April 2005 revealed that records storage leader Iron Mountain had fallen victim to the loss of tapes containing sensitive customer information. Because of this incident, Iron Mountain said in its statement, "Iron Mountain is advising its customers that current, commonly used disaster recovery processes do not address increased

requirements for protecting personal information from inadvertent disclosure." They further went on to advise, "Iron Mountain, therefore, is recommending that companies encrypt backup tapes containing personal information..." and ended by saying, "We believe encryption is the best way for businesses to meet the increasing need for privacy protection.

### Today's Regulations Are Tomorrow's Jail Sentences

Still, while most organizations perform backup data and maintain offsite copies, backup tapes remain largely unencrypted. This leaves the risk at high levels and exposes both the company, the IT managers, (and even supervisors of these departments not directly related to a breach), to stiff fines and penalties for failure to comply with government regulations that control exposure of confidential consumer information, such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Fair and Accurate Credit Transaction Act of 2003 (FACTA), and the Financial Services Act of 1999 (Gramm-Leach-Bliley or GLBA).

With so many different regulations, one would assume the rules are clear-cut and the playing field is level. Savvy corporations understand the regulations and know exactly what to do to reduce their risk, right?

## Best Practices for Securing Your Backup Data

---

Unfortunately, as with all new regulations, there is much work to be done in plugging the holes, but one thing is clear: it doesn't matter whether the breach is accidental or intentional. If it happens to you, you're responsible.

While the overall purpose of these regulations is to create effective internal controls, detect unauthorized use, enforce system maintenance, provide the necessary information for forced independent audits, and prevent corporate fraud, the bulk of the decision making is still left up to the individual IT organizations, with stiff penalties for those in the line of fire. Particularly at risk is the DBA who, because of high-level access to data, can be found most legally liable if a breach should occur.

### **Stay Out of Jail With the Newest Encryption Hardware**

Although the process of data backup and encryption is not the behemoth it once was, many IT department heads still struggle with the concept. It is commonly agreed among IT professionals that truly complete encryption can take years to implement. There is, unfortunately, nothing straightforward about implementing these new procedures but, thankfully, new encryption methods and hardware are helping to take away some of the difficulties commonly associated with the process of encryption.

What can be done to ensure the security of this data and protect those involved with it? What, if anything, is holding your organization back from taking the necessary steps to choose the only appropriate solution, data encryption? Which encryption solution best meets your needs and will instill the highest level of confidence?

It's no longer about user availability of backup tapes. The bigger issue is now is the confidentiality and integrity of your data. With news about security breaches hitting the airwaves in greater numbers every day, the issue of encryption is not going to go away. With the newest regulations taking shape as you're reading this, the risk to you personally is just too great. No longer is it a matter of whether you're going to encrypt, but when and, even more importantly, how.

## Best Practices for Securing Your Backup Data

---

One excellent solution is the Paranoia family, hardware appliances for tape backup encryption that fits in seamlessly with your current environment, takes little time to setup and has little to no effect on current backup procedures.

The Paranoia2 painlessly solves several of your most pressing encryption issues, lessening your risk even when you don't have all the IT staff you would like. The Paranoia2 seamless interface adds a critical component of security and meets your biggest challenge by not interrupting your workflow or your network's performance.

Access to data through this secure hardware appliance now means there's only one way in, making it nearly impossible for your data at rest to be vulnerable to attack from an unknown source. As difficult as the transition from simple backup to encryption can be for some to grasp, there's simply no going back. Previous backup methods are woefully inadequate and new regulations are fast catching up to ensure the level of security so necessary

### About the Author

Paul Howard is joint founder and managing director of DISUK Limited. Mr. Howard was trained in the Royal Air Force where he specialized in cryptography. During his time with the RAF, Mr. Howard served both in Europe and the Middle East as well as a tour at HQ Strike Command. After leaving the RAF, Mr. Howard played key roles within major UK Electronics Groups. Founded in 2004, DISUK Limited is a British company specialising in design and manufacture of electronic data storage encryption systems.

---

DISUK Limited  
Silverstone Innovation Centre  
Silverstone  
Northamptonshire  
NN12 8GX  
United Kingdom

Tel: +44 (0) 1327 856070  
Fax: +44 (0) 1327 856071

Web: [www.disuk.com](http://www.disuk.com)  
Email: [Sales@disuk.com](mailto:Sales@disuk.com)

Copyright © 2007 DISUK Ltd. All rights reserved.



The trademarks, logos and service marks ("Marks") displayed herein are the property of DISUK or other third parties. You are not permitted to use these Marks without the prior written consent of DISUK or such appropriate third party.

All other trademarks mentioned in this document are the property of their respective owners.