Security of Backup Data

May 2005

Tommy Ward, CISSP
Principal, MSB Associates

Introduction

If your company is like many others, you have put a lot of effort into securing your information systems. You've implemented technology and procedures at great expense, but you may be omitting an important last step: secure off-site storage.

From firewalls and strong authentication to intrusion detection and anti-virus, you have defense in depth through a variety of technologies and procedures. You also have a back-up system that schedules backups from the critical servers and copies the content to tape. Just to make sure that you can survive a disaster, you also store those tapes off site. If you are like thousands of others, you wait for to the guy that shows up at the loading dock on Tuesdays. If he's wearing the right t-shirt and carrying a clip board that he asks *you* to sign...you hand over those tapes with all of your most important data on them, and expect that, when you need them, the guy will bring them back.

As common sense and recent headline grabbing events would indicate, this process deserves a little more thought. Backup procedures are not simply an IT issue, but are an important part of corporate risk management and governance. Part of our job as security professionals is to challenge assumptions, to anticipate potential problems, and to propose solutions to avoid or mitigate those problems. This paper examines some assumptions about backup, and outlines ways to address common risks.

> Recent losses of backup tapes have been reported at Ameritrade, Bank of America and Time Warner. The costs of poor retention of corporate data have been mounting as well, with Time Warner footing the bill for one year of Credit Watch for 600,000 current and past employees and dependents. Morgan Stanley was ordered to pay $1.45 Billion to Ronald Perelman, in part because it failed to produce all relevant email during the disclosure phase of the trial.

Potential Risks

A very generalized assumption made across almost all industries is that backing up data from production systems onto some archival media is an important part of business continuity. Making backups, and using tape drives for archival is the de facto standard. Most people don't even consider alternatives to this process, although disk drive technology has evolved to the point where disk based storage is more cost effective than tape storage. For quite some time, we in the security field have known that off site storage of backup tapes introduces some level of risk to the confidentiality of the data which is stored on those tapes. Let's outline some of the potential confidentiality risks:

Storage media in the possession of the delivery driver may be lost. This could happen

from simple human error, as is believed to have happened in the Ameritrade and Time Warner cases. Once physically lost, we have no control over access to the content.

Storage media may be stolen from the delivery truck. Even if the truck is locked while the driver is inside the building of another customer, the truck could be stolen or burglarized. Of course, any serious data thief would probably consider an unmarked van an easier target for burglary than a corporate data center. Once again, if stolen, we lose control of access to the data.

Storage media on the return trip from the centralized storage site may be delivered to the wrong customer. Often the tape containers are unmarked, or only numbered or marked with a barcode. A routine and repetitive manual process such as driver delivery of these tape containers is susceptible to error. If mis-delivered, we are at the mercy of the recipient to respect the confidentiality of the data.

The delivery driver may act alone or in collusion with others to divert tapes. While most backup storage services perform screening and background checks on their employees, employee misdeeds are certainly possible. Most of the pickups and deliveries are performed by a single employee, making detection of abuse much more difficult than if two employees were dispatched in each truck. Finally, the centralized storage facility itself may be compromised through inadequate physical security or through lapses in employee screening by the off-site storage provider.

Whether by accident or intent, these various scenarios represent potential threats to the confidentiality of our data.

There are a few availability risks as well, for example:

- In the previous scenarios, not only is the data on the tapes potentially accessed without authorization, but the tapes are no longer available for use in the event that a system restoration is required.

- The tape system needed to restore from the backup tapes could be destroyed in the same event that necessitated the need to restore systems (fire, flood, etc.)

- The delivery truck may not be able to reach your facility, in the case of a widespread local or regional catastrophe such as hurricane, flood, earthquake or terrorist attack.

Mitigation

Companies should choose mitigation strategies based on a risk assessment, taking into consideration the likelihood of each risk occurrence, the potential impact, and the cost of

the mitigation effort. Often the most significant component of mitigation cost is increased labor resulting from the modified procedures. Because of this, it is important to perform this risk analysis in a way that encompasses all related operational procedures and asset protection.

A number of steps can be taken to manage and reduce the risks that result from your decision to outsource the off-site storage of backup tapes containing critical data.

1. *Carefully scrutinize contracts with the off-site backup provider*. While the selection of a provider may often be based on cost and availability of service in your area, the fact that this provider will have physical possession of your most valuable corporate assets warrants extra diligence. As with any outsourced IT service provider, you should seek audit rights, assurance that the service provider's hiring procedures include criminal and credit background checks on all employees and indemnification of losses. Sadly, the largest service providers may resist these commitments, leaving you to bear all of the risk resulting from mistakes made by you or the service provider.

2. *Use locked containers to transport your tapes*. While no easily portable container can withstand a serious effort to access the tapes within, locks will discourage casual perusal, prevent another customer from inadvertently loading your tapes onto their system if wrongly delivered, and provide an obvious indication if unauthorized access to the tapes has occurred.

3. *Encrypt the contents of all data prior to writing to backup tapes*. Some commercial backup systems provide encryption as a feature. Depending on the amount of data involved, in-house backup scripts can be used to perform encryption on a backup server, using well known cryptographic applications such as PGP/GPG or even custom developed applications based on RSA BSAFE® or the popular OpenSSL libraries. For larger amounts of data, dedicated cryptographic hardware may be required to reduce the encryption time. In all cases, key management and key recovery are important considerations. If the keys needed to decrypt the data are only available on the backup machine, the entire backup process may prove useless if that original backup machine is lost in the same incident that causes the need for restoration from tape (fire, flood, etc.)

4. *Selectively encrypt only sensitive data*. For example, consider an on-line shopping site having a very large product catalog database, all of which is already public data, as well as application and operating system code that may not be sensitive. Customer data, including names, addresses, authentication credentials and possibly credit cards or bank account numbers or other financial data would also be present. The time and processing cost needed to encrypt just the sensitive customer data would probably represent a fraction of the time and processing

[] RSA and BSAFE are registered trademarks of RSA Security, Inc.

needed to encrypt all data in the system. This simple example illustrates the benefit of selective encryption, but to apply this approach to enterprise backup procedures requires that a current and accurate data classification scheme be in place.

5. *Encrypt data at rest*. This phrase refers to is a requirement addressed in the financial world by the Gramm-Leach-Bliley Act (GLBA) and in the health care industry by the Health Insurance Portability and Accountability Act (HIPAA). Once again, a current and accurate data classification scheme is needed to drive this implementation of encryption of data at rest, but if this has been done consistently throughout the organization, encryption of backup data is not as important.

These mitigation steps can be taken independently or together to address confidentiality risks. Unfortunately, they do not address availability risks. There is another approach that addresses both problems.

Site Diversity

Rather than send copies of your data to an off-site storage provider, keep the data on your own machines and on your own network. This sounds like a step backward in terms of disaster recovery, but not if you have multiple sites in different geographic areas. If your company already has operations at one or more locations, consider implementing remote on-line storage across those locations for backup. Tape handling can be reduced or eliminated, which effectively addresses much of the confidentiality risk inherent in shipping tapes to and from the off-site storage location. Because the data is on-line, on a network that your company controls, access does not depend on a vendor's ability to get trucks on the road. Additional benefits include increased flexibility in backup schedules, and reduced delay in retrieving stored data to restore a system.

This approach also takes you one step towards having an alternate operational site for the applications you host. In the best case, site diversity can be part of a load balancing strategy across one or more locations. This way your company achieves not just redundancy but improved performance from its investment in backup systems. If your company operates at a single location, consider the use of a co-location or disaster recovery 'hot site' facility geographically distant from your corporate site for this purpose.

Site diversity is not a panacea, however. It introduces issues of connectivity and data transport bandwidth that must be carefully considered and planned for.

Creating a Corporate Strategy

Backup procedures are an important part of assuring that your company can continue to do business in the event of a system failure, and as part of a larger business continuity plan to address loss of facilities. Ideally, the backup strategy should be based on a risk analysis which considers the value of various resources to the business, the business impact of loss or disruption of those resources, and both the cost and effectiveness of various procedures in mitigating the business impact. Often, backup of desktop and departmental functions may be left to the local departments, while backup of mission critical and corporate systems should be handled as a corporate issue. Addressing the confidentiality of data backed up for those mission critical systems is often overlooked, but should be an integral part of the overall strategy. Rather than implementing or continuing to use procedures that have been based on standard practices over the years, the assumptions which led to use of those practices should be examined, and where they are no longer valid new practices should be developed.

Conclusion

Backup failures have gotten high-level attention and media exposure recently. Many organizations will react to these publicized events and implement some form of encryption of their backup tapes. A few will proactively use the heightened awareness of this problem to initiate a thorough risk assessment and carefully design a system that addresses as many of their business continuity needs as possible with the least cost and impact on operations.

MSB Associates provides assessment, design and integration services to its clients, and is ready to assist in selecting the secure backup systems appropriate to a variety of corporate IT contexts. If your company needs assistance in any of these areas, please contact us at info@msbit.com.