



# White Paper

## Enterprise Tape Encryption Requirements for the Banking Industry

By:

Jon Oltsik  
Enterprise Strategy Group

August 2006

# Table of Contents

<b>Table of Contents</b> .....	<b>i</b>
<b>Executive Summary</b> .....	<b>2</b>
<b>Banking 2006: Highlighted by Rapid Change</b> .....	<b>2</b>
Data Security: Another Banking Priority .....	3
<b>Data Security and Tape Encryption</b> .....	<b>4</b>
Today's Tape Encryption Options Are Limited .....	5
<b>Tape Encryption Must Become a Service</b> .....	<b>6</b>
Outboard Encryption .....	6
An Enterprise Tape Encryption (ETE) Architecture .....	6
<b>IBM Does ETE</b> .....	<b>8</b>
Key Management Is the Key .....	8
IBM's ETE Architecture at Work .....	8
<b>The Bottom Line</b> .....	<b>10</b>

## Executive Summary

Banking isn't what it used to be. Between globalization, increased competition, the demand for innovative products, and new technology implementation, the banking industry is changing at least as fast as any other industry. As business models rapidly advance, banks are also challenged to comply with a growing list of government regulations demanding tighter process controls and greater data security. This paper concludes:

- **It's all about the data.** Successful banks will be the ones that collect, analyze, and share market data in order to understand consumer trends, create new products, and outsource non-core business processes.
- **Today's data security measures lag behind.** In the process of capturing, using, and storing new data, many banks aren't doing a very good job at keeping it secure as measured by the number of data breaches in the last year (over 300 publicly disclosed data breaches in the United States between February 2005 and the middle of August 2006, source: privacyrights.org). This is true in many areas but it is especially pronounced with regard to tape data. Without secure tape encryption processes and technologies, off-site backup rotation, records retention, and partner data exchange are at risk of a data breach.
- **What's needed is a combination of outboard encryption and a services-based tape encryption architecture.** Today's tape encryption solutions can't deliver the scale, flexibility, or price performance requirements for the banking industry's high volume requirement. What's needed is a new type of enterprise tape encryption architecture that places cryptographic processing on the tape drives themselves, provides enterprise encryption key management, and makes encryption a distributed service rather than an all-in-one solution.

This type of solution is now available from IBM based upon its IBM System Storage TS1120 tape drive, combined with flexible key management options for the enterprise.

## Banking 2006: Highlighted by Rapid Change

The early 21<sup>st</sup> century has certainly featured rapid technology, economic and business changes. In this whirlwind of activity, no sector has been impacted more than the banking industry. Some of the unprecedented challenges include:

- **New customer demands.** Until recently, consumer banks were based on volume, offering a limited number of products to a large number of customers but this business model is now obsolete. Banking customers are extremely well informed and are very selective, so banks must adopt a mix of volume-based and customized offerings. With the continued increase in Internet connectivity and consumer-focused tools, satisfying the whims of consumers will only become more difficult in the future.
- **Frenzied Competition.** The passage of the Riegle-Neal Interstate Banking and Branching Efficiency Act of 1994 and the Gramm-Leach-Bliley Act of 1999 led to a wave of banking mergers and acquisitions. As of the end of 2003, the 25 largest banks and savings institutions held 56% of total industry assets (source: FDIC). There has also been a corresponding increase in global expansion as industry leaders like the Royal Bank of Scotland, Deutsche Bank, and Citibank compete at home and abroad. These activities segment the market in super one-stop-shopping banks, industry specialists, and non-

bank entities offering consumer-focused financial services.

- **Specialization.** Even the largest global banks are finding it difficult and expensive to compete for finicky consumer business in every market with every product. Since bigger isn't necessarily better, many banks are approaching their businesses with a much more "layered" approach by choosing the business activities in which they excel and outsourcing many back-office and operational support tasks. Bridge Bank of Northern California is an example of this layered banking strategy. Bridge Bank competes for business in the tech-centric Silicon Valley and outsources almost all of its IT needs.

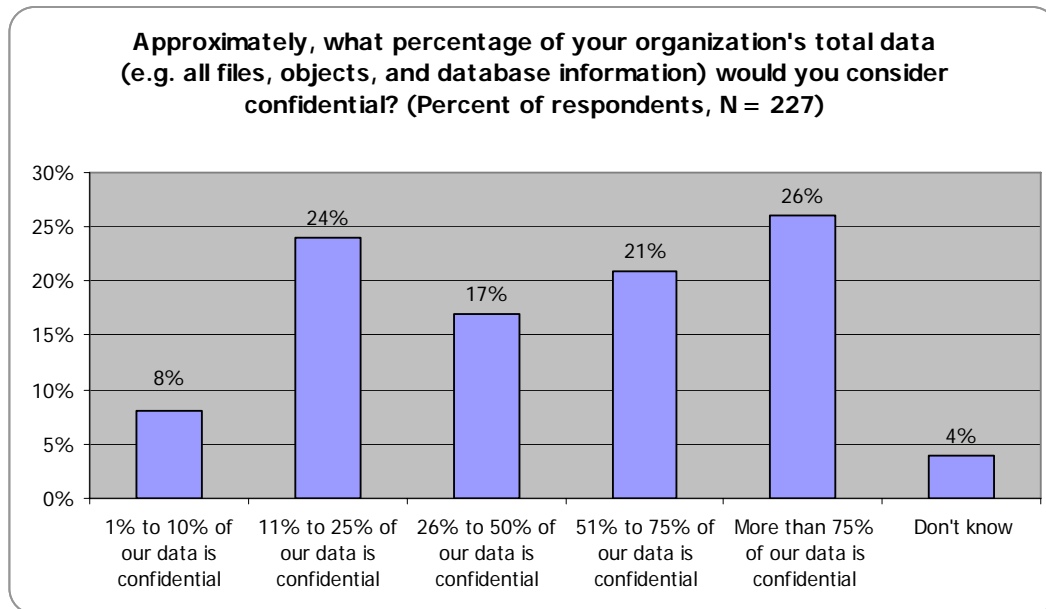
While revenue growth is driven by the creation of new on-line products, profitability is a function of automating manual tasks and lowering transaction costs. These activities place an enormous emphasis on the IT department. Banks must be able to assess performance metrics, monitor consumer behavior, and develop new products in rapid fashion. In order to keep up, banks must collect, analyze, and share their business data in new and creative ways on an ongoing basis. It is fair to say that in today's competitive market, the data tail actually wags the banking dog.

### Data Security: Another Banking Priority

While capturing, analyzing, and sharing business data, global banks must also be more attuned to data security than ever before. Banking and securities regulations like Basel II, GLBA, and various SEC 17a-4 force banks to adopt higher levels of risk management, secure private data and retain critical records for long periods of time.

This may seem like a simple requirement but it is actually extremely difficult because private data is everywhere. According to ESG Research, most security professionals at large organizations believe that at least 50% of their total data capacity could be considered confidential (see Figure 1). This confidential data ubiquity challenges even the best IT shops with issues like:

**Figure 1. Large Organizations Consider Most Information Confidential**



- **Visible data breaches.** In the United States alone there have been over 300 publicly disclosed data breaches between February 2005 (ChoicePoint breach, 2/15/2005) and the middle of August 2006 (source: [privacyrights.org](http://privacyrights.org)). These breaches have resulted in

embarrassing headlines, unexpected costs, and the exposure of over 90 million American citizens' private data.

- **IT operations efficiency.** Yes, there are tools available for regulatory compliance management and confidential data security but many are one-off point solutions that require an army of IT administrators to manage. Banks need enterprise-class central solutions that provide protection and efficient command-and-control.
- **Business process integration.** If there is one certainty related to security it is that business processes always trump security countermeasures. Said another way, business managers realize the need for improved security but they don't want to force their employees or business partners into modifying existing business processes in order to interject protection. Security must be seamless or it will likely be rejected outright.

Clearly, the banking industry is walking a fine line. On one hand, banks must continuously react to rapidly changing market conditions, focus their business models, and collaborate with business partners. On the other, they must increase security and oversight to protect valuable data assets and adhere to government regulations. Succeeding in this climate demands shrewd risk management and picking the right battles.

## Data Security and Tape Encryption

Historically, security solutions were implemented on a tactical basis in response to the threat *du jour*. SPAM problems demanded gateway SPAM filtering devices, spyware proliferation called for desktop spyware scanners, and so on. This type of knee-jerk security process was adequate in the early days of Internet connectivity but it can't meet the needs of today's fast-paced banking industry. To balance security needs with business objectives, banks must seek out enterprise-class security solutions that fit into existing business and IT processes with minimal disruption.

One area that fits this type of enterprise security context is tape encryption. Once regarded as unnecessary overhead, banks now see tape encryption as a critical security countermeasure. Why? Because tape encryption can help:

- **Alleviate the risk associated with data breaches and disclosure.** Of the publicly disclosed data breaches described above, there were a total of 18 publicly-disclosed data breaches as a result of lost/stolen backup tapes leading to the exposure of private data of over 9 million Americans (Source: privacyrights.org). Three of these incidents impacted some of the largest banks in the world, exposing the records of over 7 million American citizens! ESG estimates that the cost per lost record ranges from \$25 to \$150 to fund activities like customer notification, credit protection services, and account number changes. Obviously, the numbers can add up quickly (see Table 1).

**Table 1. Potential Costs Associated with Data Breaches Resulting from Tape Loss/Theft**

Number of lost records resulting from three major tape loss/theft	Potential cost @ \$25 per record (low cost per record watermark)	Potential cost @ \$150 per record (high cost per record watermark)
7.1 million	\$177,500,000	\$1,065,000,000

- **Protect the confidentiality and integrity of archival data.** Many regulations mandate records retention periods of a decade or more. Tape media is often used for records retention. Surprisingly, this data does not simply sit around and collect dust. According to ESG Research, 42% of organizations claim that they were involved in a legal or

regulatory inquiry that necessitated a search for and/or retrieval of electronic records. Tape encryption is necessary in order to keep archived data confidential and tamperproof.

- **Enable secure data sharing amongst business partners.** Banking success depends upon continuous data exchange and savvy data analysis amongst business partners. While most inter-company transactional data rides across global networks a lot of bulk data is still shipped on tape. Since tape-based data exchange often contains regulated private data or valuable intellectual property, it must be protected with strong encryption.

### Today's Tape Encryption Options Are Limited

Tape encryption may be more important than ever in the banking industry but it is also nothing new. In the past, there were three primary options for tape encryption, each with its own strengths and weaknesses (see Table 2):

1. **Software-based encryption.** Many backup software packages and storage utilities provide an option for tape encryption as part of their feature set. Software encryption can be adequate in a limited fashion but it can also greatly increase server CPU utilization and severely hamper backup performance. Given this restriction, few users adopted software-based alternatives.
2. **Host-based encryption.** Enterprise systems like IBM's System z provide dedicated crypto-processors that can off-load encryption tasks from core memory and system processors. Many users find this option attractive, particularly for SSL/TLS encryption for Internet-based applications. But the high volume tape encryption required for archiving and data backup can over extend core system resources.
3. **Appliance-based encryption.** As cryptographic processing advanced, a number of vendors introduced tape encryption appliances that sit in the data path and encrypt the bits as they pass by. Appliances are a great turn-key solution but they can be expensive to own and operate. Appliances also have a scalability ceiling as they can only support 5-6 drives each.

**Table 2. The Strengths and Weaknesses of Existing Tape Encryption Options**

Encryption Option	Strength	Weakness
Software-based encryption	Widely available today from backup software vendors	Increase CPU utilization which can greatly impact performance.
Host-based encryption	Dedicated crypto-processors off-load overhead from main memory and CPU.	Not well suited for high-volume data encryption
Appliance-based encryption	Turnkey solution for encryption and key management	Expensive to purchase. Can only scale up to 5-6 tape drives per appliance.

Historically, these tape encryption weaknesses were tolerable since tape encryption was extremely limited. Now that tape encryption has become a requirement these limitations could become a real bottleneck. In order to maintain business practices while protecting data security, banks simply need a better solution.

## Tape Encryption Must Become a Service

Tape encryption limitations resemble numerous other IT problems of the past. Stand-alone solutions can't scale, so more and more systems are needed. This leads to high cost and operational overhead. Like other IT areas in the past, what's needed is a solution based upon specialized distributed services. ESG believes that this solution is made up of two components: 1) Outboard Encryption, and 2) An Enterprise Tape Encryption Architecture.

### Outboard Encryption

Advances around cryptographic processor packaging, design, and price/performance are driving a new type of tape encryption solution that features outboard encryption. With outboard encryption, cryptographic processing occurs on the actual tape drives themselves. This subtle change actually addresses all of the shortcomings existing encryption options. Outboard encryption:

- **Off-loads cryptographic processing from host CPUs.** Since all encryption operations take place on the tape drives it is transparent to backup servers. In initial testing of the IBM TS1120, outboard encryption had no measurable impact on tape drive performance, meaning backup windows are not impacted.
- **Extend encryption to all connected hosts.** Since encryption takes place at the tape drive, the TS1120 can encrypt data coming from any connected host. To take advantage of this capability, drive-based encryption services can be integrated into backup software, storage utilities, tape libraries or operating system policies.
- **Scale performance across tape drives.** With outboard encryption, scalability is a function of the number of tape drives. This eliminates the need to add multiple appliances and change configuration parameters in order to boost performance.

Outboard encryption is especially useful in the rapidly changing banking industry. With the increasing amount of data needed for market analysis, outboard encryption can help banks scale their needs over time. Outboard encryption scalability is also important for maintaining backup performance service levels in the midst of ever-increasing storage capacity.

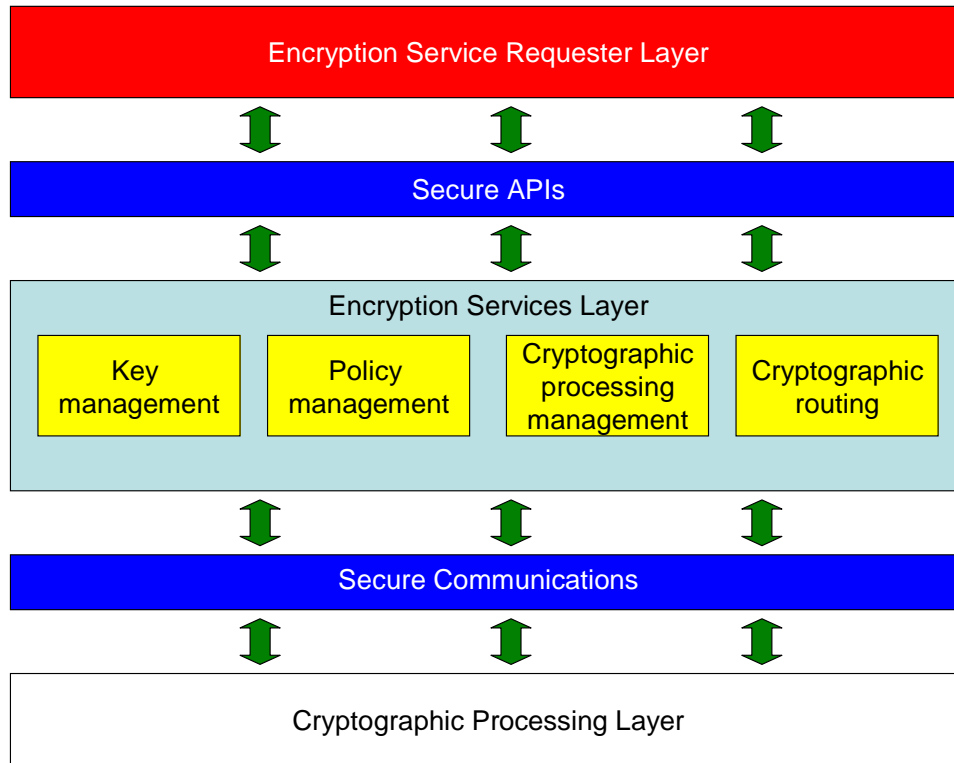
### An Enterprise Tape Encryption (ETE) Architecture

Traditional tape encryption was based upon all-in-one solutions performing cryptographic processing, key management, and policy management. Outboard encryption enables a new architecture based upon distributed encryption services. ESG calls this architecture Enterprise Tape Encryption (ETE). The ETE architecture is composed on three discrete layers (see Figure 2).

- **Encryption service requester layer.** Various systems (i.e. file systems) and applications (backup applications) that need to encrypt data can call the encryption services layer and relay which data needs to be scrambled. Aside from this call, the tape encryption process is completely transparent to requester layer systems and applications. When a backup application wants to restore encrypted data, the encryption services layer will intercept this request, perform the necessary operations to decrypt the data, and then pass it along.

- **Encryption services layer.** The ETE services layer acts as the workhorse of the architecture and masks the complexity of enterprise tape encryption from applications and devices. To accomplish this goal, the ETE encryption services layer serves as a

**Figure 2. The Enterprise Tape Encryption (ETE) Architecture**



middleware bridge between encryption requesters and cryptographic processors by providing services for key lifecycle management (i.e. key generation, key protection, administration, etc.), policy management, logging/reporting, and actual cryptographic processing.

- **Cryptographic processing layer.** Actual encryption operations can live anywhere in the infrastructure. When any cryptographic processor receives a request to encrypt data, it subsequently calls the key management server and asks it to generate an encryption key. Once it receives an encryption key from the key manager it performs the requested cryptographic operations. In this way, the cryptographic processing layer also acts as a service but remains dormant much of the time. When called to encrypt data, it wakes up and works with the encryption services layer to execute cryptographic operations based upon specific policies.

ETE is similar in nature to SOA, a popular software architecture in the banking industry. Given the services-based architecture of ETE and the distributed nature of systems and devices in a typical enterprise banking infrastructure, the goal of ETE is to provide flexibility for any-to-any tape encryption requirement. For example, a backup system could ask for encryption services from any available drive in a tape farm composed of multiple libraries. Likewise, an archiving system could encrypt large files to a set of remote tape drives in a secure location. This also allows for changes over time. As new servers, backup applications, and tape drives are added

across the enterprise, they can join the ETE process because it is controlled by the ETE services layer rather than hard-wired into specific systems.

## IBM Does ETE

Yes, there are many tape device manufacturers that provide outboard encryption or plan to do so soon. What separates IBM from the pack is its ability to provide a complete and extensible ETE architecture (see Figure 3), including an enterprise key management capability.

The IBM tape encryption solution utilizes outboard encryption on its recently released TS1120 tape drives which aligns with the ETE cryptographic processing layer described above. The TS1120 acts as an encryption service -- encryption requests can come from servers that use the TS1120 (including mainframe, UNIX, and Linux systems). The TS1120 tape drives perform the encryption based on data encryption keys passed to it from a separate key manager service that can act as a single central control point on behalf of the enterprise. Key management services can reside on the mainframe, or on a server with AIX, i/OS, Linux - even HP-UX or Sun Solaris. This service-based approach makes the IBM solution very flexible for different enterprise configurations.

### Key Management Is the Key

Generating, storing, and distributing encryption keys is one of the biggest challenges associated with tape encryption in a distributed ETE architecture. To provide this type of architectural solution, IBM offers a Java-based program that is highly portable, and is supported on many different platforms. In simple terms, the software generates and communicates encryption keys to the TS1120 tape drive and stores the public/private keys in a server-specific key store.

IBM's ETE architecture also supports the notion of key management as a service. IBM's Encryption Key Manager (EKM) can run on a different server than the server running the tape application. For example, the EKM can run on z/OS, even though the tape drives are encrypting data using a TS3500 tape library attached to an open systems server. In this case, customers can use their mainframe as their central tape encryption key manager.

ESG believes that mainframes may be particularly well-suited to provide centralized key management services for a number of reasons. To maximize key management availability, customers can leverage the highly-available Parallel Sysplex to avoid single points of failure for the key data stores. Key management also benefits from the security-rich features of the mainframe. With centralized key management is on z/OS, clients can take advantage of the same crypto hardware that's been protecting ATM networks for the last decade. They can also use the time-tested security products for authentication, authorization auditing and PKI services. Finally, clients can integrate into many of the existing mainframe management processes such as robust disaster recovery of their key information.

For non-mainframe data centers, there is another optional encryption option provided by IBM's Tivoli Storage Manager (TSM) which has the ability to fully manage and exploit the use of outboard encryption. This provides one stop shopping for the TSM customers.

### IBM's ETE Architecture at Work

In IBM's ETE architecture, the actual tape encryption is handled in the TS1120 tape drive. Each tape cartridge has a unique AES symmetric data key. The data key itself is protected by a public key of an asymmetric key pair generated by the Encryption Key Manager. The public-key

encrypted data key itself is written on the tape. This process is the same as an SSL handshake. Only the public/private keys are kept in a host key store.

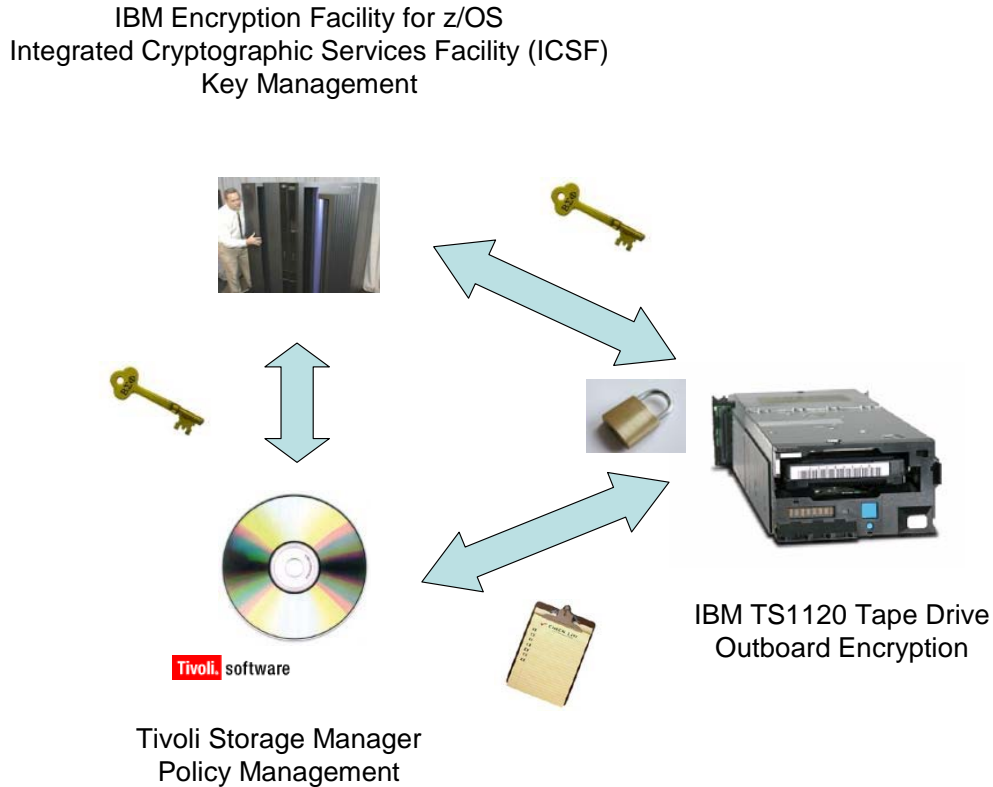
This type of key management, modeled after SSL, makes the IBM solution very scalable, allowing customers to manage keys for hundreds of thousands of encrypted tapes over years or even decades of operation. It also makes the key management fairly simple, both in the number of keys that needs to be kept track of, and in being able to leverage the same security processes that may already exist for their network security.

In summary, IBM's introduction of the TS1120 gives it an immediate position of leadership with ETE solutions. Customers can benefit from:

- **A high performance and easily scalable cryptographic processing layer.** With outboard encryption on the TS1120, IBM can provide an ETE architecture that maintains high volume backup and archival performance. Scalability is a matter of adding in new drives to distribute the encryption load over time. This also eliminates the need for add-on specialized encryption hardware.
- **Common key management services.** TS1120 drives can call key management services on mainframes, open systems platforms or TSM. Large enterprises may find z/OS integration especially attractive since the TS1120 can interoperate with existing key management, mainframe administration, and security facilities.
- **Transparent implementation.** Since TS1120 tape drives reside at the "end of the line," encryption functionality can be added to backup, archive, and data exchange applications and processes without the need for custom integration or massive operational overhead.

From a business perspective, IBM's ETE offerings will not disrupt business operations with burdensome technical requirements. And since these products work with existing systems and processes, they will deliver low total cost of ownership. Finally, IBM ETE will immediately enable data privacy protection and partner data exchange. In this way, IBM's solution can enable the business, not just safeguard IT assets.

Figure 3. IBM ETE Architecture Based Upon the TS1120



## The Bottom Line

To compete in the 21<sup>st</sup> century, the banking industry is moving its business model at lightning speed. Unfortunately, this rapid change is being offset by regulatory compliance and data security issues. Banks are challenged to find solutions that can support their business processes while enhancing data privacy and protection.

There are a myriad of areas involved in this process but it is important to prioritize activities and solutions that deliver the highest return. While it may not be the sexiest topic, tape encryption fits within this category.

To overcome the limitations of current tape encryption solutions, ESG recommends:

1. Outboard encryption performed locally on tape drives for linear scaling.
2. An Enterprise Tape Encryption (ETE) architecture, including encryption key management, for application integration and secure key management.

With the recent addition of its TS1120 tape drive, IBM offers hardware, software, and services needed to build an ETE architecture. Smart CIOs will certainly place IBM on their short list of ETE vendors.