

TRACKING STORAGE SECURITY

Executive Summary

By now, government executives clearly understand the importance of securing sensitive data in multi-level, multi-user environments, although there's still much confusion about federal regulations, as well as which storage security offerings to choose and how to adequately fund such projects.

In a July survey of 124 government executives created by NeoScale Systems Inc., and conducted by GCN Research Online, nearly 80% reported data is being transmitted and stored in multiple environments and shared with different organizations. Up to 70% of respondents have either deployed or are evaluating at least one storage security solution.

Of the regulations related to use of storage encryption, the greatest percentage (42%) reported their workplaces are largely in compliance with the OMB's MO6-16 regulation. In general, however, 40-50% of respondents said none of the listed regulations are applicable to their storage encryption strategies, which to some degree indicates a lack of awareness. At the same time, at least 28% said their workplaces are nearly in full compliance with all listed regulations.

Of the respondents sharing sensitive data, a majority (58%) reported data is being exchanged internally within government agencies, clearly indicating a need for storage encryption. Another 20% said data is also shared externally with government contractors, raising additional security concerns.

Respondents have deployed an average of two solutions to address storage security and most plan to deploy at least one more. The largest

percentage, 40%, have deployed file system-level encryption, while 36% already use storage security appliances, and 35% have backup applications using software-based encryption. Of the choices listed, 36% of respondents said column-level database encryption was being evaluated for future use.

In this survey, 46% percent of respondents were from civilian agencies and 54% worked in defense agencies. In terms of job function, 37% worked in systems and network management, followed by 23% in technical management and R&D, and another 23% in executive/command positions. In some cases,

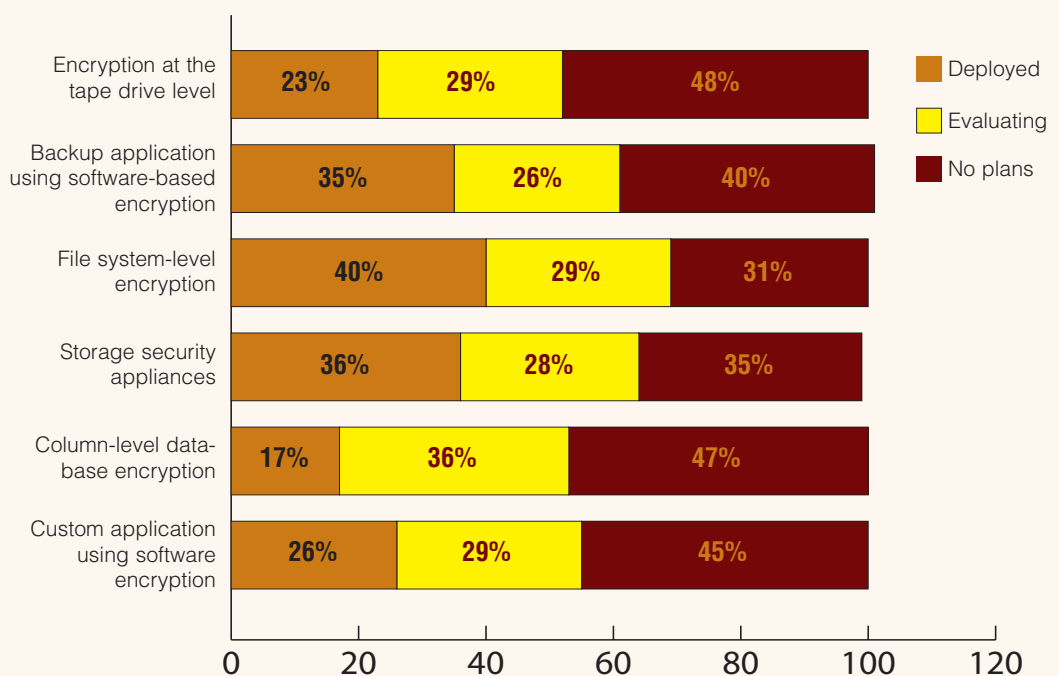
the total number of responses exceeded 124 because executives were asked to check all that apply.

Other interesting findings include:

*While 41% of respondents said they have no plans to deploy a global/hierarchical key management system to manage the keys of individual storage security endpoints, about half reported they have either deployed (19%) or are evaluating (29%) such a system.

*The top two environments considered important to secure were 'open system (Windows, UNIX, Linux) disk,' mentioned by 57%, and 'file encryption systems,' selected by 54% of respondents.

Have you deployed or do you plan to deploy any of the following types of storage security solutions?



Source: GCN Online Survey, July 2007

Global Key Management is the Cornerstone of Storage Security

Ongoing compliance challenges of federal regulations such as FISMA, HIPAA, HSPD-12 and the Office of Management and Budget's MO6-16, along with embarrassing headlines about lost or stolen data, are altering the way federal IT organizations view data protection.

Because a vast majority (80%) of GCN survey respondents are now sharing data within and across agencies, they may also be starting to realize the need for a more strategic plan to holistically manage storage security, as they grapple with systems and storage devices that may not interoperate.

Until now, addressing the most critical needs, such as securing mobile data and backing up sensitive information to offsite tape storage devices has occupied federal IT departments. What's most needed now, however, is help in meeting demands for scalability and compliance with federal regulatory storage management mandates. Indeed, government organizations are discovering they must not only secure, archive and manage enormous data volumes, but also the disparate key management systems already in place, which is why half of the GCN survey respondents said they are evaluating a key management solution.

In many ways, global key management could really make a difference. Global key management is used to create, maintain, protect and control the keys used to encrypt and decrypt data. It represents a solution to the growing headache of managing the rapid proliferation of storage security devices implemented over the last several years, to address the need to safely share sensitive information. As security requirements have grown, government organizations are realizing a need for centralized control over key management, along with the tools to archive and vault those keys to enable seamless backup and recovery.

NeoScale Systems Inc., Milpitas, Ca., launched the first open global key management system, called the CryptoStor KeyVault, in March 2006. Designed to manage keys from storage encryption devices such as tape drives, storage security appliances and backup applications, KeyVault provides centralized control for managing the keys used to encrypt data. The product automates and secures the archiving and recovery of keys,

ensuring that encrypted data can be recovered at a secondary disaster site, or in the event that a local key management system is lost. KeyVault can be deployed across all locations, providing a single key management service for all types of data at rest operations.

Beyond key management, however, the GCN survey also underscored the growing importance of file encryption, mentioned by 54% of respondents as a top concern. File encryption is crucial to controlling access to files outside an agency's sphere of influence, although NeoScale understands that encryption alone doesn't offer sufficient protection against data loss or theft. The ability to share files in a controlled and secure manner, both within and outside an organization, remains a continuing ordeal. To accomplish this goal without significantly changing existing file sharing network infrastructures and without being required to re-educate users is an enormous challenge. That's why NeoScale is currently working to provide centralized security management that will ensure correct usage of encrypted files, while automating key sharing to allow files to be accessed from any location, by only those users authorized to do so.

Currently, NeoScale boasts nearly 300 customers, including a fifth of the Global Top 50. Through rigorous testing with leading storage and security partners, NeoScale expands the interoperability of its storage security solutions with applications and tape/disk products. NeoScale provides an open, standards-based global key management platform to unify storage management across disparate systems and storage devices. NeoScale also works with organizations such as the IEEE P1619.3 committee to drive standards for key management interoperability.

NeoScale can help government organizations securely and safely share information, by providing centralized storage security controls, automating key management and hardening both key archiving and auditing to meet ongoing compliance obligations.



For more information, please visit www.neoscale.com
or call (408)473-1303.