THE CLIPPER GROUP
Voyager™

Navigating Information Technology Horizons℠

Published Since 1993 Report #TCG2006014 March 7, 2006

When the Data Demands Discretion — DISUK Encrypts the Tape

Analyst: Anne MacFarland

Management Summary

There will always be a role for tape is a homily usually said with some degree of condescension – but, as enterprises become more far flung, more outsourced, and more unwieldy in their use of video and other large, sequential data assets, the statement becomes more widely (if sporadically) true. The convenience of the network, so familiar to us as users, is not universal. Our demands are light, and we are, for the most part, on the pulling end. It's like assuming your *front-end* experience at a Mom and Pop grocery store would work on a wholesale distribution scale. It could – and at farmers markets it does, sort of – but the success of a farmer (the one pushing the goods) rests on the high volume push of commercial contracts as well as a face-time presence at market day. For many businesses, there are similar high volume pushes of data that turn a profit – or complete a process. These pushes over distance are scheduled, not executed in real time. They must be totally secure and accomplished at minimum cost.

Besides the lure of profits and the pursuit of efficiency, another significant factor that shapes business process is *PARANOIA*, as expressed in the adage: *It is nice to trust but better not to.* Many business owners sleep better by expecting the worst. This approach treats IT systems as inherently unreliable – because, sooner or later, some portion of them will be. It treats networks as insecure because, as our government has shown us, targeted data capture is possible – and with XML headers, it will become easier. It treats the enterprise as inherently distributed because, sooner or later, whether by acquisition or because of disaster, it will be. If, as a default, you plan for the worst case, most surprises are pleasant.

In the current climate of alliances, partnerships, and the physical dispersal of organizations, sharing data over distance is unavoidable. **If it is large volumes of sequential data that your company is sharing, the network approach is not the only option. Encryption of removable media, done properly, is another option.** DISUK, Ltd., based in Silverstone, UK, takes this approach and perfects it with a tape encryption turnkey appliance, aptly named *PARANOIA2*. Why tape? *Because tape can transport data without unnecessary co-mingling and exposure on telecommunications links.* Optical disk (UDO) will be supported later this year, with a similar rationale. Why encryption? *Because accidents happen.* And, why appliances, rather than a network approach? *Because, to the paranoid, avoiding risk is the cornerstone of a good solution, and simplicity is the safest framework.* For more details, read on.

IN THIS ISSUE

The Global Pervasiveness of Risk

Business data contains information that is sensitive, ranging from business strategy data to product development and pricing data, to feedback on operations and marketing campaigns – and, of course, customer data. Misuse of sensitive information extends well beyond the highway robbery of account numbers. Longer-term nefarious schemes, like moles or embezzlement, can debilitate enterprise strategies while leaving little evidence of their existence.

Information use in the enterprise has a long tail that is in some areas quite broad. The lifecycle of the sensitivity of data may be different from the lifecycle of its use. A good bit of business information is always sensitive. What a business does, who its customers and suppliers are, and its intellectual property, does not change, and does not become less confidential over time. Other sources of business information may not contain overtly sensitive information, but it is still not what you would want advertised on a street corner. Moreover, even if the information is not sensitive, the fact that information that was not publicly available has been stolen saps organizational confidence.

The Basics of *PARANOIA*

PARANOIA2 is a solution that does not try to meet technology's equivalent of *political correctness*.

The appliance is a proprietary box.

PARANOIA2 has been selling commercially since 1996. What it does is your business, but how it does, it is not. The interfaces are open – which is all you need to know. It can accommodate almost any kind of enterprise tape – from the early 8 mm systems to LTO 2 and 3, IBM 3592, and STK 9840. It connects to SCSI, Fibre Channel, or iSCSI. It does not support ESCON or FICON connectivity, but will in response to customer demand.

This is an accessory, not a participant in the network.

Reporting (via SNMP) is optional.[1] If the power is disconnected, *PARANOIA2* will maintain internal keys for up to an hour (you can set the parameters based on your local situation), and then will destroy the keys in it, presuming that prolonged power loss means it has been stolen. As the customer, you will have stored a separate copy of the keys elsewhere. Perhaps on tape or on a thumb drive stored in a safe deposit box - something that does not rely on power for permanence. If a disaster happens, you can buy another appliance, install it at a new site, insert the key data, and it will happily decrypt the tapes. Everything is under the control of the enterprise.

A Solution for the Nomadic Power User

You may think that the limousines for senior executives are merely a sign of status, but they also secure the executives' laptops that are chock full of sensitive information. If your company has power users who need large data sets and sensitive information but don't always go the limousine route, a *PARANOIA2* appliance and a terabyte (compressed) tape cartridge can let the worker carry all the data he or she needs with perfect safety.

The use of encryption and removable media does require a certain discipline. Nevertheless, the popularity of (usually unprotectable) thumb drives shows the continuing popularity of removable media. DISUK gives a solution similar in approach to a thumb drive, though admittedly a bit more unwieldy.

Service Providers and PARANOIA2

In data producing environment, *PARANOIA2* sits in front of a tape drive. On the receiving end, it is not necessarily as clear-cut a proposition. Your payroll service provider, for example, services many accounts, probably using the same drives with different tape cartridges. If the service provider has made the choice to use DISUK to enhance its tape-based business, all well and good. Use of an encrypting appliance such as DISUK's PARANOIA2, with separate keys for each account, does ensure that data from different organizations is never co-mingled, and that the accounts never get confused – which to the paranoid organization may be a selling point. DISUK's products can integrate with existing encryption key management products. However, if the service provider does not embrace encryption, the DISUK appliance may be seen as an intrusion.

[1] DISUK does offer another product, *SafeTape*, which is a tape subsystem rather than a turnkey solution. It is not discussed in this bulletin.

Pricing

PARANOIA2's base price is around $14,000 (subject to the variability of currency exchange rates). Most PARANOIA2 customers are multi-site companies that buy multiple appliances.

Why A Simple, Local Solution May Be Just What Your Organization Needs

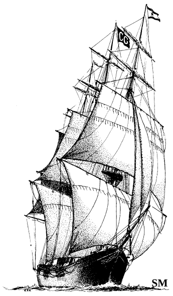
Developments in cyber crime and competitive cyber-intelligence may make physical isolation, that last bastion of security, important again. The viruses and malware we hear about are the public surface of a very large iceberg. Risk avoidance is a more effective strategy than risk mitigation.

If you are a small organization, and your data transfer headaches are relatively few but very painful, the DISUK approach may be attractive. In such cases, the DISUK appliance and courier or overnight shipping may be less expensive than network-based encryption and telecommunications costs for bulk data transfers, particularly if they are across national borders.

For most businesses, operational efficiencies to meet needs for revenue come first. Directly behind them comes the need to mitigate unacceptable risks – that cannot be avoided. Only then can you plan for the future. Risk mitigation is not a matter of revenue – though it becomes one if you do not do it. Therefore, you mitigate risk tactically, where you need it. For many companies, the transfer of bulk data is a risk begging to be mitigated.

Conclusion

In these days of massive networks, rampant virtualization, many organizations are constrained by the massive ramifications of whatever they do. It is beneficial to pause and look at a specifically focused, simple, non-network solution, targeted at a specific vulnerability. If *Keep It Simple, Stupid* (KISS) is the approach you crave, and your risk is data exposure, DISUK's *PARANOIA2* may be just what you seek.



About The Clipper Group, Inc.

The Clipper Group, Inc., is an independent consulting firm specializing in acquisition decisions and strategic advice regarding complex, enterprise-class information technologies. Our team of industry professionals averages more than 25 years of real-world experience. A team of staff consultants augments our capabilities, with significant experience across a broad spectrum of applications and environments.

➢ ***The Clipper Group can be reached at 781-235-0085 and found on the web at www.clipper.com.***

About the Author

***Anne MacFarland* is Director of Data Strategies and Information Solutions for The Clipper Group.** Ms. MacFarland specializes in strategic business solutions offered by enterprise systems, software, and storage vendors, in trends in enterprise systems and networks, and in explaining these trends and the underlying technologies in simple business terms. She joined The Clipper Group after a long career in library systems, business archives, consulting, research, and freelance writing. Ms. MacFarland earned a Bachelor of Arts degree from Cornell University, where she was a College Scholar, and a Masters of Library Science from Southern Connecticut State University.

➢ ***Reach Anne MacFarland via e-mail at Anne.MacFarland@clipper.com or at 781-235-0085 Ext. 128. (Please dial "128" when you hear the automated attendant.)***

Regarding Trademarks and Service Marks

The Clipper Group Navigator, **The Clipper Group Explorer**, **The Clipper Group Observer**, **The Clipper Group *Captain's Log***, **The Clipper Group Voyager**, and *"clipper.com"* are trademarks of The Clipper Group, Inc., and the clipper ship drawings, *"Navigating Information Technology Horizons"*, and *"teraproductivity"* are service marks of The Clipper Group, Inc. The Clipper Group, Inc., reserves all rights regarding its trademarks and service marks. All other trademarks, etc., belong to their respective owners.

Disclosure

Officers and/or employees of The Clipper Group may own as individuals, directly or indirectly, shares in one or more companies discussed in this bulletin. Company policy prohibits any officer or employee from holding more than one percent of the outstanding shares of any company covered by The Clipper Group. The Clipper Group, Inc., has no such equity holdings.

Regarding the Information in this Issue

The Clipper Group believes the information included in this report to be accurate. Data has been received from a variety of sources, which we believe to be reliable, including manufacturers, distributors, or users of the products discussed herein. The Clipper Group, Inc., cannot be held responsible for any consequential damages resulting from the application of information or opinions contained in this report.