



How to Fully Protect Your Storage Environment

Like anything else in your organization, there are vulnerabilities that can lead to serious business risks within your storage environment. It's only a matter of time before something on your network is savaged by attack. A solid plan to prevent your data from threats is critical.

This E-Guide from SearchStorage.com explores the many components of storage security. Learn about solutions, trends, methods and considerations to be aware of, through expert articles that explain:

- The inevitability of tape encryption
- Why and how your storage environment will be attacked
- How to encrypt your storage

Read this E-Guide to find out where you're at risk and how to prevent it.

Sponsored By:

Quantum[®]



How to Fully Protect Your Storage Environment

Table of Contents:

[Hot Spots: The inevitability of tape encryption](#)

[Why and how your storage environment will be attacked](#)

[Storage encryption: How much is enough?](#)

[Resources from Quantum](#)

Hot Spots: The inevitability of tape encryption

Jon Oltsik

You can't duck it any longer; it's time to encrypt your backup tapes.

When I joined the Enterprise Strategy Group (ESG) approximately four years ago, we had a burning suspicion that the storage layer of the technology stack wasn't very secure. Our day-to-day conversations with IT professionals reinforced this hypothesis, but that wasn't enough. Early in 2004, we embarked on a quantitative research project to compare our thoughts to real user data. Chalk one up for data and statistical analysis; this time we weren't just reading our own headlines, we were spot on.

ESG concluded that while the entire storage infrastructure was extremely vulnerable, one of the most ominous weaknesses was tape encryption. When enterprises (i.e., organizations with 1,000 or more employees) were asked if they encrypted backup data, only 7% responded "Yes, always." A startling 60% of storage professionals said "No." This meant that the preponderance of data on tape was being carted to some offsite storage facility in cleartext, a proverbial accident waiting to happen.

Acceptance is growing

What's taken place since our initial study? There's good news and bad news.

When ESG Research revisited this topic in 2006, we found that 25% of enterprises had deployed tape-encryption solutions, 14% planned to deploy tape encryption in the next 12 months, and another 21% had no plans to deploy tape encryption but were interested in the technology.

I'd love to say ESG drove the behavioral change, but my guess is that it was related to three critical factors:

1. **Visible data breaches.** In February 2005, Bank of America lost backup tapes containing the personal information of 1.2 million customers. The same thing happened to Citigroup in June 2005, only this time the tapes contained the personal data of 3.9 million customers. ESG estimates a per-record cost of between \$30 and \$150, which is a total cost of approximately \$1 billion to more than \$6 billion for the two breaches combined. Obviously, these incidents demonstrated that the risk of outsiders gaining access to backup tapes was real.
2. **More privacy laws.** The granddaddy of U.S. privacy laws has the catchy name of California Senate Bill (SB) 1386. SB 1386 mandates that companies publicly disclose data breaches if any California citizen's private information is exposed. In effect, SB 1386 was behind the Bank of America and Citigroup disclosures. As of this writing, a total of 28 states have passed similar privacy laws, and there are more stringent regulations in effect in Europe and Asia.
3. **Boardroom jitters.** When CEOs see data breach headlines emanating from Bank of America and Citigroup, they tend to be more willing to open the corporate wallet to scramble bits on their tapes.

Tape encryption falls under the category of “mobile data,” information with the ability to leave the building. This has become the focal point of encrypting data at rest, and it’s why ESG is seeing steady investment in laptop and tape-encryption tools.

Most still don’t encrypt

Despite all of this progress, 75% of enterprises still don’t encrypt their backup data. Why? Some are still hung up on the traditional objections—cost and performance—to any form of encryption. Enterprises may not have a budget for backup encryption or may feel that encryption will add too much overhead, slow down backup processing and throw a monkey wrench into an already tight backup window. Another obstacle to backup encryption is user confusion—encryption is still a black art to many storage professionals. Finally, storage managers can quickly assume a “deer in the headlights” look when confronted with a choice of encrypting backup tapes using backup software, file-system tools, cryptographic appliances or switches, or encrypting tape drives.

In spite of the fact that three-quarters of enterprises continue to eschew backup encryption, IT managers have become resigned to the inevitability of encryption technology. They recognize that the next LTO drive they buy will have encryption capabilities, while future disk arrays will support the Trusted Computing Group (TCG) storage security standards. The tape-encryption infrastructure will arrive within the next 24 months, whether you like it or not.

Given the certainty around tape encryption, organizations should begin their tape-encryption planning as soon as possible. Based on countless enterprise interactions, ESG recommends large organizations anticipate tape-encryption best practices through the following:

Assess risks. If you work in a regulated industry at a publicly traded firm where backup tapes are shipped offsite with a third-party service provider, you face a high degree of risk. Fast track a decision and proceed to implementation as soon as possible. If your organization doesn’t fit this precise profile, you should still undertake a thorough risk assessment. For example, many firms entrust employees to deliver tapes from one data center to another. In cases like that, policy creation, signed employee agreements and background checks may be a logical first step toward safeguarding tape-based data. Make sure to assess future privacy legislation and international laws that may impact any near- or long-term plans.

Take a backup inventory. There are four basic options for tape encryption: software (i.e., backup software), file-system encryption at the media server, an encryption appliance or switch, or encrypting tape drives. Before choosing one, assess all backup technologies, amortization schedules and backup architectures. Which equipment is due for an upgrade? Is tape backup used as a primary or secondary backup medium? Be selective but open-minded; many large organizations will end up with a heterogeneous encryption architecture that includes more than one of these technologies.

Map tape-encryption plans to backup strategies. Encrypting tapes might not make sense if your organization plans to implement virtual tape or disk-to-disk backup in the near future. In that case, disk-based encryption may be a better fit.

Consider other tape applications. Tape may become the preferred medium for e-discovery and records retention, digitizing historical information or deep archival. Much of this data may be considered private or “company confidential,” and it may also be regulated. If that’s the case, do a risk assessment to see if encryption is required.

Get to know the chief information security officer (CISO). In terms of security, check with the CISO to see if the security team has any future plans for centralized encryption key management. If so, you may want to explore internal integration options and query vendors about their key management road maps. Remember that key management may also introduce some extremely tight processes that impact day-to-day operations. As the Boy Scouts say, “Be prepared.”

The bottom line

In the near future, encryption technologies will closely mirror the old “death and taxes” cliché as one of those things that are inevitable. Approximately 25% of enterprises are there, but the vast majority are still on the sidelines. ESG recommends a proactive plan toward encryption that includes risk assessment, technology inventory, implementation planning and coordination with the security team. It’s better—and cheaper—to be safe than sorry.

About the author: *Jon Oltsik is a senior analyst at Enterprise Strategy Group as well as the founder of its Information Security service in 2003. Oltsik is now widely recognized as an expert in security management and technology and also focuses on identity and access management.*



Transport Data Securely Between Sites With Quantum's Disk & Tape Encryption Solutions

Transporting backup data between sites can be challenging, whether you use tape or want to replicate data across the wire. Quantum disk and tape solutions offer encryption options, giving you the flexibility to choose what's best for you. Quantum DXi-Series disk-backup systems incorporate de-duplication and fully-encrypted replication, allowing you to securely link sites for enterprise-wide backup and disaster recovery. Quantum Scalar libraries, combined with Quantum Encryption Key Manager (Q-EKM) and LTO-4 technology, provide secure, non-disruptive encryption for your tape environment. Quantum solutions enable you to meet required levels of data confidentiality, integrity and availability across distributed environments. Backup, Recovery, and Archive. It's what we do.

www.quantum.com/encryption

Why and how your storage environment will be attacked

Kevin Beaver

Storage security vulnerabilities abound. You likely know of many and likely haven't thought about others. What's causing the problem, and what should you be looking out for? It's just a matter of time before something on the network—a router, a server, a Web application—is exploited by an external attacker or malicious insider. With the increased visibility and avenues of attack, your storage systems are no different. I'm not speaking gloom and doom, just being realistic.

How storage got pulled into the problem

Like anything else IT-related, there are vulnerabilities that can lead to business risks within your storage environment. It's not the mere fact that storage systems are susceptible to attack that makes this a big deal; nor is it related to the fact that storage security easily falls within the scope of your organization's compliance initiatives. Instead, it involves things like having to secure multiple layers of systems that support your storage environment, such as physical access, network configuration and transport, authentication mechanisms, management tools and so on. There's also the fact that various business processes, such as information classification, legal discovery, user provisioning, system monitoring and ongoing auditing, apply directly to storage.

In the past, the complexities associated with storage systems, network isolation and lack of storage knowledge have kept most attackers at bay. The tides are turning, and now the bad guys understand what storage is about and how it works. They're discovering the multiple avenues for accessing the storage environment and utilizing storage-specific hacking tools to try and get to your systems. So, regardless of what storage technologies you use and how they're configured, there's near a 100% certainty that your systems are at risk and will continue to be.

Here's why and how your storage environment will be attacked.

Common misconceptions and oversights

Regardless of how your organization's data is created, handled or otherwise processed, it will inevitably end up in your storage environment. You're going to have to be prepared to keep it locked down and inaccessible from unauthorized people the best you can. Acknowledging this fact is half the battle, especially if you work closely with your information security team or any others that are responsible for protecting electronic assets.

There are other issues that aren't quite as simple. In fact, many are outright falsehoods based on "old-school" thinking and a general lack of information security knowledge. In no particular order, here are seven issues you, as a storage administrator or manager, will have to overcome in order to keep your storage systems secure and make improvements long term:

1. Storage security does not equal redundant systems and good backups. These two elements are only part of what's going to keep your data safe and sound, so it's important not to solely rely on them as has been done in the past.

Why and how your storage environment will be attacked

2. The protocol doesn't matter. Both IP-based storage and Fibre Channel have their own unique issues and one is not necessarily any less susceptible to attack than the other.
3. Storage encryption is not the silver bullet. Not for data at rest and not for data in transit. It does offer a nice last line of defense in your network security layers, but it cannot be relied upon by itself.
4. It's not the storage team's responsibility to ultimately secure the storage environment. It's everyone's responsibility, including the information security team and other IT, audit and compliance staff. Good communication between different departments is critical to make this work.
5. Your users can/should never be trusted to do what's right. Set your users and yourself up for success by keeping them out of what they don't need access to with network segmentation and proper authentication and access controls.
6. Ability does not always equal permission. Just because a user or an attacker can access your storage systems doesn't mean they're supposed to have that access. Backdoors and users with unnecessary privileges are often overlooked and often lead to breaches. Be on the lookout for these holes.
7. A user or external attacker will likely be able to get in far enough to do damage. Contrary to popular perception, there are ways to get into your storage environment—often with ease. Do you know who has access that can lead to system compromise? The only way to know for sure is to test for storage security holes on a consistent basis.

How it will happen

When you combine the problems outlined above with your system complexities and difficulties of keeping everything within your sights at all times, this will inevitably lead to an unnecessary or unauthorized storage exposure. There are hundreds of ways for storage systems to be attacked. They'll come from within your own network and from the outside, but here are seven biggies:

1. The network perimeter or DMZ will be breached. Separating IP-based storage systems into their own secured area is often overlooked, which is a sure-fire way to facilitate an attack.
2. The internal network will be breached. Many internal LANs are configured without segmentation and proper access controls, allowing trusted insiders to poke and prod around to see what they can get to.
3. Share and file permissions will allow for unauthorized access. More often than not, it's very easy to find misconfigured share and file permissions allowing anyone and everyone to browse, load and copy data they shouldn't have access to. This is an especially serious issue when it comes to users copying files to their local drives and other parts of the network "temporarily" for the sake of convenience.
4. Management software will fall into the wrong hands. Or, your management stations will be compromised leading to unauthorized users connecting to and "managing" your storage systems.
5. DNS servers will be hacked. This allows for name pollution and redirection, and eventually users storing sensitive data to the wrong place—an attacker's system.

Why and how your storage environment will be attacked

6. Network traffic will be captured. This will happen on both wired and wireless networks allowing for man-in-the-middle attacks, session hijacking and both online and offline password attacks. This is much easier than it seems. Improperly secured wireless networks are a breeze to compromise. All it takes on the wired side is a good network analyzer and Address Resolution Protocol (ARP) poisoning via Cain & Abel or similar tool.
7. Operating system and application weaknesses will be exploited. Compromising a server is no longer theoretical, or something that can only be carried out by an external attacker with tons of knowledge and time. In fact, a simple misconfiguration or missing patch on a storage device or supporting system can be easily discovered using Nessus Vulnerability Scanner, QualysGuard PCI or similar tool. These weaknesses can then be exploited by pretty much anyone in the real world, regardless of their technical abilities, in a matter of minutes using Metasploit, Core Impact or another similar tool.

Over the years, there has been a disconnect between storage administration and information security, which has helped facilitate these storage system attacks. There's a lot of payoff associated with doing something about the problem. If you start working on fixing the underlying issues that are contributing to this within your organization, you'll be well ahead of your peers and on the path toward improving your overall storage skill set and keeping your organization's storage security in check.

About the author: *Kevin Beaver is an independent information security consultant, speaker and expert witness with Atlanta-based Principle Logic LLC. He has more than 18 years of experience in IT and specializes in performing information security assessments revolving around compliance and IT governance. Kevin has written six books, including Hacking For Dummies and Hacking Wireless Networks For Dummies (Wiley), as well as The Practical Guide to HIPAA Privacy and Security Compliance (Auerbach). He can be reached at kbeaver@principlelogic.com.*



Don't Be The Next Newspaper Headline

Over the past 3 years data breaches have cost companies millions of dollars which includes the cost of the records themselves, cost associated with notifying millions of customers of the loss, and fines and damages. Not to mention the damage it can inflict on your companies image. Quantum Encryption Key Manager(Q-EKM), was designed to provide secure non-disruptive Encryption key management for your Quantum library. Q-EKM is deemed unbreakable by the US Government and secure enough even for classified data. No matter how complex or big your enterprise, our expertise in data security will keep things safe and secure. Let Quantum secure your peace of mind.

- Utilizes industry-standard algorithms, Meets AES-256 Bit Encryption Standard (Govt. Recommended)
- Out-of-the-data-path solution—Q-EKM does not impact backup performance
- Set-and-forget design for ease-of-use
- HA (High-Availability) capable
- Now available for Quantum Scalar i2000 & Scalar i500 libraries with LTO-4 drives

www.quantum.com/encryption

Go-online today to find out more about our encryption solutions www.quantum.com/encryption

Quantum

Storage encryption: How much is enough?

Kevin Beaver

There's a lot of talk about regulatory and industry compliance these days—especially when it comes to storage encryption. Pretty much every facet of IT is affected by this in one way or another and storage systems are no exception. Many well-intended IT professionals recommend encryption as the solution for everything, but the experienced storage administrator knows it's not that simple. The bottom line is, whether it makes good technical sense or not, storage encryption may be a viable—if not the only realistic—control available to lock down your sensitive information at rest.

Before you do anything, including responding to management or auditor inquiries as to why you're not using storage encryption, you've got to determine exactly what's at risk in your storage environment and what's vulnerable when it's not encrypted. All too often, IT administrators jump on the "let's implement technical controls for the sake of security and figure out a good reason why later" bandwagon. Don't join the crowd. You need to look deeper and determine what sensitive information is stored, how it can be exploited in the storage environment (by internal and external attackers) and the consequences once it happens. A good place to start is with this related tip, [Storage vulnerabilities you can't afford to miss](#), in which I wrote about general vulnerabilities associated with storage systems, as well as in two other tips on [hacking techniques](#) and [niche tools that can be used to test for, and exploit, storage weaknesses](#).

Looking at your storage weaknesses using this method is the only reasonable way to determine what, if anything, needs to be encrypted. It's also a good way to justify budget and resources for buying and implementing new storage security technologies and provides a good source of documentation (aka CYA log) if you choose not to encrypt your information at rest.

So, you've got at least a seven-step process to go through to ensure everything's in check.

1. Classify your information or, if someone else handles this process, review your organization's most recent classification documentation to ensure you know what's important and what needs the most attention.
2. Determine where sensitive or otherwise "protected" information is stored in areas like your SAN/NAS environment(s), databases, local drives in servers and workstations, especially those susceptible to unauthorized access and theft like laptops, PDAs and other mobile devices, such as iPods and USB drives that can store large quantities of information.
3. Determine which regulations affect this information, such as the Payment Card Industry (PCI) Data Security Standard, the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), the Sarbanes-Oxley Act (SOX) and any of the numerous international privacy regulations and state breach notification laws. Check with your compliance manager/officer for this information if you're lucky enough to have one.
4. Assess your security to determine what information can be attacked and exploited with encryption not in place. Do it yourself internally or hire an outside expert that can have a fresh look at things.

5. Determine other security controls that create a layered defense or could even replace encryption as a defense mechanism.
6. Implement encryption controls where needed throughout your storage environment.
7. Last, but not least, document what you've done to determine where storage encryption is/isn't needed and how you came to your conclusions. This safety net can make or break your job.

With a few exceptions, I've always believed that information in transit is much less susceptible to compromise than information at rest. I made a strong case for that in *Securing data at rest vs. data in transit*. If you come to the conclusion that you don't need storage encryption, you've probably overlooked something—at least at the host level. There are tools available to allow anyone with physical access to a system (laptop, workstation, server, you name it) full control over the operating system and any information stored on it. This is something that I believe only encryption can solve.

Throughout this process, you'll likely determine that not everything needs to be encrypted—at least I hope so for your sake. The only way you're going to know for sure and be able to make informed business decisions is to figure out where the weaknesses are by using tools and techniques that can get to bottom of things. Beyond this, if there's ever any doubt about whether something's at risk and storage encryption isn't a viable security control, see if you can keep the information off your systems altogether. Of course, that's easier said than done, but why not start asking tough questions like "Why does it need to be here?" and "How long do we need to keep it?" You may be pleasantly surprised and end up with some very good storage risk reduction techniques you never even thought you had.

About the author: *Kevin Beaver is an independent information security consultant, speaker and expert witness with Atlanta-based Principle Logic LLC. He has more than 19 years of experience in IT and specializes in performing information security assessments revolving around compliance and IT governance. Kevin has authored/co-authored six books on information security, including Hacking For Dummies and Hacking Wireless Networks For Dummies (Wiley), as well as The Practical Guide to HIPAA Privacy and Security Compliance (Auerbach). He's also the creator of the Security On Wheels audiobook series. Kevin can be reached at kbeaver@principlelogic.com.*

The Daily News

20 Million Customer Records Lost!

Angry customers demand to know why data wasn't protected with an easy to implement encryption solution from Quantum

Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero eros et accumsan et iusto odio dignissim qui blandit praesent luptatum zzril delenit augue duiis dolore te feugait nulla facilisi. Nam liber tempor cum soluta nobis eleifend option congue nihil imperdiet doming id quod mazim placerat facit possit assum.



Encryption Without The Complexity With Quantum's Encryption Key Manager

Let's keep it safe and simple. At Quantum, we are the experts in Backup, Recovery and Archive solutions, providing data security across multi-site environments. Quantum Encryption Key Manager(Q-EKM), was designed to provide secure non-disruptive Encryption Key management for your Quantum Libraries while making the process simple to manage and transparent to your existing backup environment. Perfect if you're challenged with a complex backup environment encompassing multiple tape libraries and remote locations. No matter how complex or big your environment, we will keep things safe and secure.

- Utilizes industry-standard algorithms, Meets AES-256 Bit Encryption Standard (Govt. Recommended)
- Out-of-the-data-path solution—Q-EKM does not impact backup performance
- Set-and-forget design for ease-of-use
- HA (High-Availability) capable
- Now available for Quantum Scalar i2000 & Scalar i500 libraries with LTO-4 drives

www.quantum.com/encryption

Go-online today to find out more about our encryption solutions www.quantum.com/encryption

Quantum

Resources from Quantum



[Find Out More About Quantum Encryption Key Management- Q-EKM](#)

[Click here for More Information On Quantum Security Framework](#)

[Download the Quantum Encryption Key Management Technical Whitepaper](#)

About Quantum

Quantum is the leading global storage company specializing in backup, recovery and archive. Combining focused expertise, customer-driven innovation, and platform independence, Quantum provides a comprehensive, integrated range of disk, tape, and software solutions supported by a world-class sales and service organization.

www.Quantum.com