

contents

**Protecting
confidential data**

- 2** Backup encryption
- 9** Intrusion prevention and encryption
- 15** Laptop encryption
- 20** Database encryption

Encryption 360°

Data breaches and regulatory mandates are fueling an interest in encryption. We'll look at encryption from every angle.

BY INFORMATION SECURITY AND SEARCHSECURITY.COM

SPONSORED BY



Backup Encrypt

BY W. CURTIS PRESTON

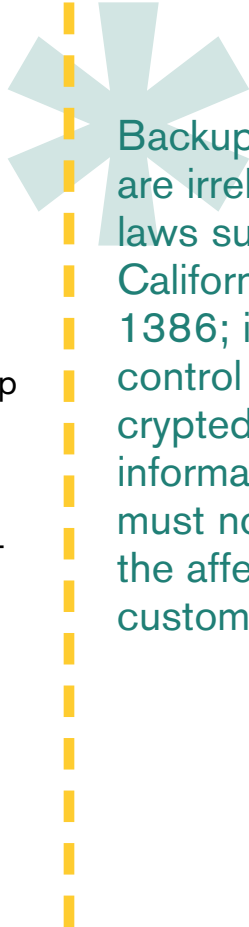
Unencrypted data at rest is data at peril.

Since **Bank of America** disclosed in 2005 that it lost a backup tape with customers' personal data, nearly 80 other companies have reported similar embarrassing mishaps. The list of organizations losing tapes with sensitive personal information includes many high-profile names: Ameritrade, Time Warner, CitiFinancial, ABN Amro Mortgage Group, People's Bank, Con Edison, the U.S. Department of Veterans Affairs and Chase Card Services. The breaches affected millions of people, resulted in millions of dollars in direct costs, and even more in indirect costs.

Direct costs include notifying customers of the breach, estimated at \$5 to \$10 per

person, and the expenses associated with controlling damage to the brand, such as advertising in national newspapers. Indirect costs stem from damage to the brand. A loss of trust can easily cause some customers to depart, or potential customers to choose another company to do business with; either way, it's lost revenue.

The key to your organization avoiding this fate is encryption, as all unencrypted backup tapes are readable by determined cyber-criminals, no matter what your vendor tells you. Some vendors claim that their backup format is proprietary and can't be read without their database and software—don't believe them. Backup formats are irrelevant to laws such as California's SB 1386; if you lose control of unencrypted personal information, you must notify the affected customers. If you can't notify them in a reasonable timeframe, you must contact the media. Several states have similar breach notification laws. As of the end of last year,



Backup formats are irrelevant to laws such as California's SB 1386; if you lose control of unencrypted personal information, you must notify the affected customers.

these laws only apply to unencrypted data. You are not required to notify anyone if the data was encrypted.

It's a clear business case for encrypting tapes that are going to leave a company's physical location. It could save your organization millions of dollars if a tape is lost, and will ensure that any damage to your brand is minimal.

LOOK BEFORE YOU LEAP

When you consider encrypting backup tapes, you need to consider the risks of encrypting stored data. They're very different from the risks associated with encrypting data in flight. If you have a problem encrypting data in flight, you know it right away and fix the problem. For example, if an application is sending data across an encrypted channel, and something happens to the encryption, the application will crash. A root-cause analysis will determine that encryption failure was the culprit.

However, if you have a problem with encrypted data at rest, you may not know it for weeks, months or years—and probably not until it's too late. This is because unlike encryption of data in flight, the read step only happens when you verify or restore

TIP

The Classification Challenge

Classifying data is tough without help from appliances tailor-made for the chore.

If an organization wants to encrypt only data that would result in it having to do a public disclosure in the event of a breach, then it needs to be concerned about personal information. The challenge is in making sure you locate where such information is stored.

Some of the obvious locations are customer information databases, as well as imaging systems where contracts are stored. Other locations may be less obvious and very difficult to find.

The best way to ensure you've found all that personal data is to use a data classification appliance. Without one, data classification is near impossible. These appliances crawl your file systems, databases, Web pages and even backup tapes, looking for metadata to classify information based on sensitivity—and always seem to find data in places you didn't think it resided.

The cost of these devices ranges from a few thousand dollars to tens of thousands of dollars, and they support several different ways to access your files, such as HTTP, NFS and CIFS. They typically are very easy to use and install.*

—W. CURTIS PRESTON

from a tape. Therefore, unless you're verifying every tape after you've written it, the only time you're going to test your encryption system is when you perform a restore—the worst time you want to find out your encryption system doesn't work.

The biggest risk with encrypting backup tapes is that you can make them so secure

that even you can't read them. If you lose your keys, or if your processes break down, you end up with unreadable backup tapes. Unfortunately, you might not discover this has happened until the moment of truth: when you absolutely need to read that tape.

This is why key management is so important. Keys will be needed any time you attempt to read encrypted data, such as when performing a restore, and access to keys by the wrong person could render your encryption system useless.

Consequently, keeping track of the keys used to encrypt data is paramount. A database is critical for tracking what key was used on what day to encrypt what data. Any time you change the key, the database must be updated accordingly. You must also control and monitor access to the key database to prevent unauthorized access.

Although secure key management systems already exist for encryption of data in flight, they don't support multiple keys associated with a single system or tape drive over different periods of time. As a result, key management systems designed for encrypting data at rest are often much less mature.

Another risk with encrypting backup tapes is failure to strike a balance between securi-

ty and usability. This is a constant battle in security circles. If you make a system too secure, it becomes unusable or difficult to manage. If it's easy to manage, it's usually not very secure. The goal here is to find a balance—making the system more secure without significantly increasing management costs, or changing the user experience.

There are three basic ways to encrypt backup data:

- Source encryption
- Backup software encryption
- In-line hardware encryption

All three will encrypt data before it's potentially lost. However, each option will have a different impact on usability and cost, which must be taken into account. For example, many would consider a method that causes the speed of all backups to slow by 40 percent, or decreases the capacity of a tape library by 100 percent, to have too great an impact on usability to be a viable option.

SOURCE ENCRYPTION

Source encryption systems encrypt the data at its source. A file system, such as Windows Encrypting File System, or a

Keys will be needed any time you attempt to read encrypted data, such as when performing a restore.

database encrypts the data stored therein. If data is stored encrypted, and it's not unencrypted when backed up, it would meet the encryption requirement of various breach notification laws; you wouldn't need to notify customers if you lost a tape with personal data on it. These systems have the added benefit of encrypting data while it's being transferred across the network. For those concerned about malicious insiders, this can be a real plus.

Source encryption systems suffer from a number of drawbacks. First, they typically impact the performance of the file system or database in question. Every file or database record must be encrypted when written, and then unencrypted when read, which can significantly impact performance.

Another challenge is key management, because each file system or database type would typically have its own encryption system and set of encryption keys to manage. Since key management is a top priority when storing data at rest, this is a big concern. If you've got several data types to encrypt, this may become a show stopper. Managing one key system is challenging enough; managing multiple key systems would be even harder.

COMPLIANCE

PCI & Encryption

The industry standard for protecting cardholder data cites encryption as critical.

The Payment Card Industry Data Security Standard (PCI-DSS) is a major initiative being enforced by Visa, MasterCard, Discover and American Express, and is designed to ensure cardholder privacy.

The PCI DSS requires that organizations protect stored cardholder data and encrypt cardholder data when it's transmitted across public networks. While the requirement for stored data is to "protect," not necessarily "encrypt," the standard does say that it believes encryption is a critical part of protecting stored customer data, in case the other layers of the security system break down.

But PCI auditors say that even with encryption and other security measures such as network segmentation, retailers and others simply shouldn't store credit card data unless it's absolutely necessary. According to the standard, organizations should keep cardholder data storage to a minimum, and should develop data retention and disposal policies.*

—W. CURTIS PRESTON

Finally, encrypting data at the source removes the compression feature of any backup system since encrypted data cannot be compressed. This would result in a 25 percent to 50 percent loss in capacity and performance from Unix, Windows and MacOS backup environments. (Hardware compression increases performance as it reduces the number of bytes actually written to tape.)

As a result, source encryption is mainly

applicable to encrypting very small amounts of data, such as a single file system or database storing personal information. It's also appropriate if you're concerned about encrypting data before it's transmitted across an unsecure network.

BACKUP SOFTWARE ENCRYPTION

With backup software encryption, the backup application encrypts the data as it's stored on tape. Most backup software products have encryption options, and a number of vendors have beefed these up in recent months.

While this solves the multiple key problem with source encryption by employing a single key management system, the key management systems employed by many backup software applications are antiquated. A few vendors have updated their key management techniques, and some have partnered with other companies to do so. Others, however, are stuck in the '80s and use systems that are easily defeated.

For example, they use a single key that has no concept of access control; if you have that key, you can read the tape. If a rogue employee gains access to the tape and the key, he or she will be able to read the tape.

If you change the key due to that employee, he will still be able to read the stolen tape that was encrypted with the old key, but you won't be able to read backup tapes that were written prior to the date you changed the key—you would have to temporarily put the old key back in place to read old tapes.

Backup software encryption will also impact backup performance since encryption done in software is very slow. Although faster CPUs and more efficient code will help, software encryption will probably always lose the speed battle. Like source encryption, backup software encryption will also remove compression from most backup systems, unless the customer uses client-side software compression that slows the backup even more.

As a result, backup software encryption, like source encryption, is mainly applicable to encrypting small amounts of data. For instance, if you have a single database that stores personal information, you could encrypt the backups of just that database. However, it can be quite difficult to identify all databases and file systems that store personal information. If you can't be sure you've identified all such databases, you'd have to encrypt all backups to make sure

Backup software encryption will also impact backup performance since encryption done in software is very slow.

you don't have to notify any customers if you lose a tape. If that were the case, this option would probably not be viable due to its impact on performance and capacity. Backup software encryption is appropriate, however, for backing up systems across unsecure networks.

HARDWARE ENCRYPTION

Another option that has increased interest in encryption is a hardware appliance that sits in the physical data path and encrypts data on its way to tape. Because the encryption is done in hardware, it can be done much faster and does not slow down the backup. In addition, encryption appliances designed for tape compress the data before it is encrypted.

These systems typically have very sophisticated key management systems that cannot be defeated by a single malicious employee. For example, they often separate the keys used to encrypt the data from the keys used to authenticate and authorize systems and personnel. They also offer features that ensure keys never get lost, such as replication and key vaulting. These systems are advanced because they were all developed within the last five years, and take advantage

of decades of lessons in data security.

The first encryption appliances available were single-purpose appliances with a few ports in and out. At the same time, encryption functionality is now being included inside tape libraries, intelligent switches and tape drives. This leads to the question: where should hardware encryption reside? As long as the hardware system compresses, encrypts and has a strong key management system, it doesn't really matter.

Hardware encryption is the most viable option for anyone wishing to encrypt a large amount of data on its way to tape. Customers can compress their backup data without any performance or capacity loss; they just need to buy enough appliances to handle their backup bandwidth requirements.

WHICH ONE?

What matters most to your business operations and which problems you're trying to solve will determine the best approach for you. If you want sensitive data to always be encrypted, then you'll want to choose source encryption. If you just want to make sure data is encrypted as it's leaving a system on its way to backup, you'll want

Hardware encryption is the most viable option for anyone wishing to encrypt a large amount of data on its way to tape.

to select backup software encryption. Just keep in mind that both of these methods have serious performance and capacity drawbacks. If you don't want to figure out what should be encrypted, and simply want to encrypt everything on the way to tape—plus avoid any performance or capacity loss in the backup system—then you'll want hardware encryption.

Whatever encryption method you pick,

it should provide some peace of mind if a backup tape goes missing. Ultimately, it's a decision an enterprise can't afford to avoid in this age of data privacy regulation.*

W. Curtis Preston is vice president of data protection at enterprise storage services firm GlassHouse Technologies, and author of *The Storage Security Handbook* and *Using SANs and NAS*.

Whatever encryption method you pick, it should provide some peace of mind if a backup tape goes missing.

Weighing the Competing Needs of Encryption and IDS/IPS

BY DORIAN DEANE & BENNY JONES

Encryption may be good for securing data, but it blinds network-based IDSes. While there aren't any surefire fixes, these techniques will steer you in the right direction.

Encryption used to be unequivocally good for security. After all, it kept the bad guys from getting at our private information, right? Who could argue with that? Many of us became crypto-evangelists, demanding encryption everywhere.

Then we realized that we were blocking our view with all this encryption.

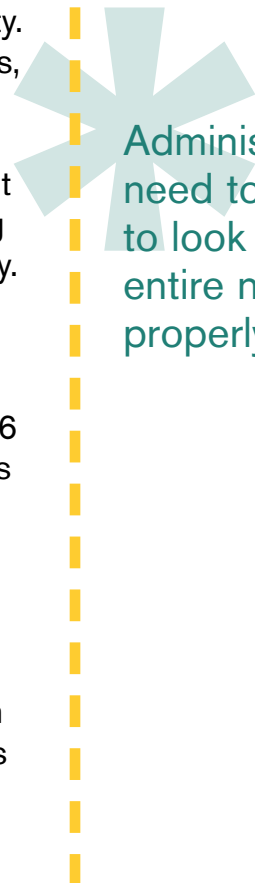
Administrators need to be able to look at the entire network to properly defend it. IDSes, IPSes, sniffer tools and network ana-

lyzers provide a clear view of network activity. But, the more prevalent encryption becomes, the more we lose that view.

So is encryption bad for security? Are IDSes and IPSes dead? No, but imprudent use of encryption can send a well-meaning network security engineer into unsafe territory.

The pressure is on for enterprises to implement encryption as a standard of due care—HIPAA mandates privacy for health care transactions, and California's SB 1386 requires the disclosure of security breaches of unencrypted personal information. In the private sector, the Payment Card Industry (PCI) security standard includes rules regarding data encryption for credit card transactions.

How can an enterprise protect itself from the bad guys, meet regulatory requirements and have an effective IDS/IPS solution? While there are no clear-cut answers, we'll



Administrators need to be able to look at the entire network to properly defend it.

explore some of the ways you can keep a clear look out for hazards on the horizon.

EVALUATING OPTIONS

Fundamentally, encryption blinds your IDSes and IPSes. Regardless of whether the IDS works through signature matching or anomaly detection, it needs to see the packet in cleartext to detect most attacks. But without encryption, confidentiality (one of the cornerstones of good information security) is reduced, if not completely lost.

While there are solutions that come close to solving parts of this problem, a balancing act is often required. Sometimes the only answer is to weigh the competing needs and pick encryption or IDS—not both.

When evaluating the options, you need to understand the importance of data privacy in your network environment. If the data is on a company's public Web site, the sensitivity is low and privacy may not be as important. However, if the data is sensitive financial information, privacy becomes paramount and encryption is likely to be one of the few practical risk mitigations.

Still, security decisions rarely hinge solely on encryption versus cleartext. If the data must be encrypted and throwing away your

IDS is unacceptable, alternatives may emerge from a threat analysis. Do you need to encrypt all the data, or just certain fields? Is the encryption intended for privacy, to prevent injection attacks, or both? Will encryption on the wire make application layer attacks more difficult?

Different solutions will present themselves depending on the threats. For example, encryption is effective at reducing threats such as TCP or UDP injection and spoofing attacks. Blindly spoofing one end of a TCP session is hard; the addition of well-managed encryption makes it nearly impossible. However, encryption is useless against other types of threats (see *"No Sure Fix," p. 12*).

SOLUTIONS

The ever-increasing number of threats to internal networks has caused a virtual stampede to encrypt corporate networks from end to end. This is laudable, but, again, we blindfold our IDS in doing so. One common compromise is to limit the use of encryption to only the less trusted portions of the path. A typical technique is to decrypt at trust boundaries (e.g., using load balancers, VPN servers, or some other front-end proxy) and resend the traffic in the clear over the more

When evaluating the options, you need to understand the importance of data privacy in your network environment.

trusted network.

This option may be acceptable when the load balancers and the endpoint servers are close, such as on the same VLAN. But as enterprise networks become larger, these edge networks become less trusted by virtue of the size of the internal networks from which they are managed. Moreover, requiring that proxies or other endpoint devices be physically close can be a design constraint. Re-encrypting the traffic before putting it back on the wire can impose significant processing requirements, but is often found in reverse-proxy architectures.

Encryption of the data itself rather than the entire communication session is another alternative. Generally, this can be decided on a case-by-case basis. The simplest example is the use of anonymous FTP to send an already-encrypted file. While FTP offers no encryption, the file itself can be encrypted beforehand. Similarly, database transactions can be sufficiently secured by encrypting only sensitive fields.

Keep in mind that a threat analysis in the context of the existing architecture may reveal other considerations. In the case of FTP, a data channel is opened that may require firewall exposures in some environ-

ments—this would clearly be a factor against using FTP above and beyond the IDS problem.

SSL Keys • If the primary threat is a non-specific inbound attack against a Web server, sharing the private SSL key of the Web server with the IDS could work; the IDS can watch the session key negotiations and decrypt the SSL streams. The benefit is clear: Attacks that may have been hidden within the SSL stream are visible to the IDS.

While this can be a workable solution, it puts the private key at somewhat more risk since it's now available on at least two hosts—the Web server and the IDS—each with its own set of vulnerabilities that must be mitigated. In some architectures, this approach can also overload an IDS, since it now carries the added burden of decrypting traffic as well as performing its normal signature checks.

While this is mostly a capacity-planning problem, it's an important one—if a key-negotiation packet is dropped during the SSL handshake, the session will be essentially invisible to the IDS. Another drawback is that this solution is not widely available for protocols other than SSL.

Keep in mind that a threat analysis in the context of the existing architecture may reveal other considerations.

IPSec AH • If the main threat is an injection or replay attack against the network connection itself, a particular form of IPSec may offer sufficient protection. Although IPSec is commonly thought to provide encryption, only the Encapsulating Security Payload (ESP) mode of IPSec actually encrypts (see below).

The other mode, IPSec Authentication Headers (AHs), doesn't encrypt the data. Instead, it uses cryptographic checksums to authenticate each packet, which prevents injection and replay attacks while leaving the data portion visible to the IDS. Although IPSec AH does nothing to protect confidentiality, since the payload remains in cleartext, it may provide an easy solution for handling less sensitive data.

IPSec ESP • IPSec ESP can provide cover for an application that doesn't use encryption; that is, all communication between two IPSec endpoints is encrypted. In some cases, this is a great solution, but there can be drawbacks.

With IPSec ESP, the choice is binary—you either allow or disallow the IPSec traffic. IPSec, by its layer 3 nature, encrypts everything; no network IDS is able to peer

TACTICAL TIPS

No Sure Fix

Encryption may seem like the perfect security fix, but it doesn't protect against everything.

Trivial passwords • A password can be guessed over an encrypted channel just as easily as over a cleartext one.

Application-level injection attacks • Once an encrypted channel is established, the application is no less vulnerable because of the encryption.

Buffer overflow or syntactic exploits • If they occur before or during the login process, your enterprise isn't covered.

Certain DoS and DDoS attacks • Resource starvation attacks will still work, as will some attacks on the crypto protocol itself.

Social engineering attempts • Technology can't protect against attacks on the user.

This is not an exhaustive threat list. Also, your encryption software may have security problems of its own. Do a quick search on critical security problems found in OpenSSH or OpenSSL to check. Nothing is without risk, not even security software.*

—DORIAN DEANE & BENNY JONES

through the crypto-armor to see what's going on inside. Thus, if your network firewall allows the IPSec traffic, it must also allow all possible TCP and UDP services between the IPSec endpoints.

Network firewalls simply cannot see inside to allow or deny specific services. And,

since it is nearly impossible to configure a functional system without several listening services above and beyond the minimum you want to provide, these unwanted service ports are exposed through the firewall.

The good news is that endpoint controls, such as host firewalls, can help reduce those problems. Most host firewalls can apply their policies after decryption to filter the undesired ports; and, more to the point, host-based IDSes can see again.

CONCLUSION

While there are no monolithic solutions to the rather vast scope of this issue, endpoint security is likely to be at least part of everyone's solution.

The history of security has shown a trend of ever-shrinking perimeters, and the natural progression of the security perimeter is to move inside to the hosts themselves. This is particularly true of firewall technology: It was once sufficient to protect the perimeter of the enterprise; later it was sufficient to have zones of higher security inside the corporate perimeter; and now, firewalls are often installed directly on the hosts.

The same logic applies to IDS technology. End-to-end encryption is desirable, and, by

applying IDS checks at the endpoint, it is less critical that a network IDS see the traffic in midstream.

An endpoint IDS solves several fundamental problems because it can look at the packets after decryption, thus largely avoiding the blind IDS problem. An oft-mentioned drawback is that if something does get past the IDS, it's already on the host—ideally, you'd like to get a warning while the intruder is still scratching at the front door.

This problem also plagues network IDSes because, in practice, there is so much low-level attack noise that it drowns out warnings of a more determined attack. Host IDSes suffer far less from background noise. Also, the detection of a scan behind the firewall, unless it comes from an authorized source, will draw an administrator's attention. At the network perimeter, the same scan would likely go unnoticed.

The biggest problem with moving security to the endpoints may be more social than technical. Few organizations are staffed or empowered to effect a lot of oversight at the level of the individual host; their domain consists of the wires and the packets that run over the wires.

One solution may be for IT workers who

The history of security has shown a trend of ever-shrinking perimeters, and the natural progression of the security perimeter is to move inside to the hosts themselves.

are closer to the application's requirements to take responsibility for deciding specific IDS rules for hosts while security departments mandate a baseline for host IDS signatures. The security department then takes on an oversight role for rules added locally by the application owners.

With perimeters shrinking, applications fighting their way through firewalls and IDS efficacy being hampered by a pandemic of false positives, organizations are evolving to respond to these trends, but security remains a balancing act. What's important to remember is that encryption carries its own set of risks. Preservation of confidentiality is nearly always a desired goal, but it is not free. And, the cost isn't just a few extra CPU

cycles to encrypt a packet—it can be as high as a crippled IDS and a well-hidden attack vector into the network.

We aren't just hiding network activity from the bad guys—we are hiding it from ourselves. While encryption remains one of the key pillars of information security, network and security engineers need to understand the consequences of its usage and find ways to ensure that it doesn't become a roadblock.*

Dorian Deane, CISSP, is a security manager, and Benny Jones, CISSP, is a senior security engineer. Both work in the telecom industry.

Preservation of confidentiality is nearly always a desired goal, but it is not free.

Laptop Encryption

BY LISA PHIFER

New business initiatives mean new threats. Are you ready?

From January to August of this year, the Identity Theft Resource Center tracked 449 major identity thefts. According to the Ponemon Institute, 45 percent of such breaches result from missing laptops. At an average corporate cost of \$197 per compromised record, why doesn't every company encrypt laptop data?

"Worldwide, about 20 percent of laptops are encrypted," says mobile security vendor Credant Technologies. "A year ago, one barrier was budget, but most companies have now gotten past that. During the VA incident, envelopes alone to notify those affected cost \$11 million. Encrypting that data

would certainly have cost less."

Stone believes that many companies do not yet encrypt laptop data because they have not determined exactly what they must do to comply with regulations and make their organization secure. "Measure twice, cut once applies to encryption," he says.

BOOTING UP

Today, most companies that encrypt laptops start with a mandate. "Ten years ago, our customers made IT-initiated point decisions," says Gerhard Watzinger, CEO of SafeBoot, which also secures mobile devices. "Now, the No. 1 driver is compliance, with corporate-wide rollouts initiated at the board level."

Alexandra Kim, executive director of ISS technology at George Washington University, experienced this firsthand.

"It's an idea we've had for years, but a 2006 board meeting gave us a turbo



Forty five percent of identity theft breaches result from missing laptops.

charge,” she says. GWU then created a five-phase plan to encrypt all confidential data with Utimaco SafeGuard. “We segmented the population and did those at the top first. Our first phase covered all users who access confidential data and carry laptops. Our next phase will encrypt all desktops in departments that use confidential data.”

Highmark Blue Cross/Blue Shield in Pennsylvania found motivation aplenty to encrypt thousands of laptops and desktops. “We’re a DoD (Department of Defense) contractor; we’re also bound by HIPAA and SOX,” says Chris Kashner, desktop specialist. “We see other companies losing data and didn’t want our name in the headlines.”

To address those concerns, Highmark deployed GuardianEdge Hard Disk Encryption, first to laptops, then to teleworker desktops. To stop flash drive leakage, Highmark later added Pointsec Media Encryption.

THE RIGHT TOOL

“**Ours is definitely** not a one-size-fits-all policy,” says Kashner. “We initially chose AES full-disk encryption for laptops because it was bulletproof. We chose [a different platform] for removable media protection because of the vendor’s DoD history, cen-

tralized control and ability to make use-case exceptions.”

San Antonio-based Clarke American Checks combines Computrace LoJack for Laptops with PGP Whole Disk Encryption on about 700 laptops. “Those programs now go out the door with all new laptops,” says senior IS auditor Deron Means. Clarke evaluated half a dozen products before settling on PGP. “If all we wanted was disk encryption, any could have done that. But most could not encrypt emailed .zip files or archives—features that were huge for us.”

The Hershey Company chose SafeBoot Device Encryption for transparency, ease of use and small footprint.

“Demonstrating audit compliance and integration with our identity management infrastructure was important to me,” says Dan Klinger, manager of IS. “Our support center also required delegated roles and central management through one console.”

Coverage can also play a big role. “If an employee buys a laptop, we have a standard,” says Rob Marti, director of IS at Integris Health in Oklahoma City, “but physicians go out and buy the latest toys; I can’t dictate what they’ll use. The faster we can support new devices, the better.”

Demonstrating audit compliance and integration with our identity management infrastructure was important to me.”

Dan Klinger,
manager of IS,
The Hershey Company

Integris chose Credant Mobile Guardian as a common file/folder encryption platform for Windows laptops, Palm PDAs and Windows Mobile 5.

WORKING OUT THE KINKS

These companies selected different platforms to meet varied requirements, but all emphasize the importance of pilot programs to work out any kinks.

“My laptop’s BIOS had to be flashed before encryption worked,” says Means. “Now we have a process of running scandisk and upgrading BIOS before installation.”

To avoid problems on older laptops, Means installs software LoJack before encryption. “You may decide to just encrypt newer laptops with chip-based LoJack,” he says.

Highmark also started slowly to minimize impact, but found that data could be encrypted reliably without extraordinary measures. “Backups and BIOS updates are fine ideas, but if you’re encrypting 4,000 laptops, it’s just not feasible,” says Kashner. “We didn’t do any of those things, and our failure rate was minimal—out of 13,000 desktops, we lost maybe one.”

“As long as the laptop itself is well managed, we don’t have encryption issues,”

says Integris’ Marti. “But on PDAs, we do a hard reset, install Credant, then reinstall applications, because some Mobile 5 devices have issues with releasing memory.”

PROCESS, PROCESS

During its pilot, GWU emphasized communication. “I personally called the head of each department before we started,” says Kim. Just two problems were encountered and both were aborted without data loss, instilling confidence required for a larger rollout.

The pilot also produced a process. “We found that encryption can take two to eight hours,” says Kim. “Now we work with departments to pick a time that doesn’t impact their business.”

Indeed, everyone interviewed identified people rather than technology as the most essential ingredient.

“Securing data is one thing; retaining the inherent usability of a device is another,” says Credant. “You can’t require users to change the way that they work. Don’t require the IT organization to change the way that they work either.”

According to Watzinger, about 35 percent of SafeBoot’s customers use both full disk

“Backups and BIOS updates are fine ideas, but if you’re encrypting 4,000 laptops, it’s just not feasible.”

Chris Kashner,
desktop specialist.
Highmark BlueCross/
Blue Shield

and file/folder encryption on the same laptop. “When you have an outsourcer administering the CEO’s laptop, you need to give him access but stop him from seeing sensitive data,” he says.

“After standardizing devices, the biggest thing is having executive management support on who gets encrypted and why, so that you’re not fighting that on a daily basis,” recommends Marti.

“We put some weight around our laptop

protection by making policies heavier,” says Clarke American Checks’ Means. “Now, if theft is due to negligence, it could cost you your job. One guy had his laptop stolen twice and he no longer works here. After that, it’s amazing how few laptops are stolen.”*

Lisa Phifer is vice president of consulting firm Core Competence and has written extensively about network infrastructure and security technologies.

“We put some weight around our laptop protection by making policies heavier. Now, if theft is due to negligence, it could cost you your job.”

Deron Means,
senior IS auditor, Clarke
American Checks

TACTICAL TIPS

Strategies for Preventing Laptop Data Leaks By Lisa Phifer

A poll by vendor Credant Technologies Inc. found that 88% of employee laptops carry sensitive information; everything from patient, customer and employee records to intellectual property, financial data and passwords. Between business risks, security breach headlines and regulatory compliance, companies have plenty of motivation to use encryption as a last line of defense against data leaks that result from laptop theft or loss. But which laptop encryption approach would work best for your company’s workforce?

ENCRYPTED PASSWORD DATABASES

Programs that selectively encrypt usernames, passwords, account

numbers and related tidbits have been available for years. Consumers who do not already encrypt their personal data should seriously consider free programs like Password Safe and KeePass. But this ad hoc approach is of little utility to employers because it depends on inherently unreliable users to decide what should be encrypted and when. It cannot ensure that sensitive data always gets protected, and thus cannot prove that private data was never exposed.

FILE AND FOLDER ENCRYPTION

To meet those needs, most businesses will choose IT-administered stored data protection, based on file/folder encryption, full-disk encryp-

tion or some combination thereof. File/folder encryption is also selective, but encrypts files automatically, based on defined attributes like file location (e.g., folder), file type (e.g., spreadsheets) or source application (e.g., everything Excel touches).

For example, the Windows Encrypting File System (EFS) is Microsoft's basic file/folder encryption tool. It can be centrally activated by using Active Directory Group Policy Objects to encrypt specified files or folders. However, EFS still relies on sensitive data being written into protected locations, and cannot stop users from copying encrypted files to unencrypted locations (e.g., thumb drives).

More sophisticated file/folder encryption products do more. For example, some offer stronger policies that make data leakage less likely, provide reports that document compliance after a laptop goes missing and can apply a consistent encryption platform and policy to heterogeneous devices, e.g. PCs, PDAs and removable storage.

FULL-DISK ENCRYPTION

For general purpose computers, the other popular approach is to simply encrypt everything stored on a physical disk or a logical volume. The goal is to ensure that nothing is ever written to storage without being encrypted. That includes not only sensitive user data, but also application and operating system files.

An example of volume encryption is the BitLocker feature in Windows Vista.

It divides a PC's boot drive into an unencrypted boot volume and an encrypted operating system volume, which is unlocked and verified at boot time using a Trusted Platform Module (TPM) chip, USB key or recovery passphrase. But data written to non-OS volumes is still unprotected, although it can optionally be encrypted using EFS.

More comprehensive full-disk encryption (FDE) scrambles the entire hard drive's contents, including boot sectors, swap files, OS files and user data. Authentication, encryption, provisioning and reporting capabilities vary, but enterprise FDE products offer features like Windows single

sign-on and central logging for security audit and compliance reporting.

COMPARING ALTERNATIVES

The main weakness of file/folder encryption is the possibility of data leakage. So why doesn't everyone use full-disk encryption? For starters, encrypting an entire disk can take hours—not including the time required to make a full system backup first. Thereafter, all data will be encrypted “on the fly,” slowing overall system performance to some (not necessarily noticeable) degree.

Some FDE pre-boot authentication methods interfere with other programs that may also be used on the protected system, from asset-tracking products to sign-on processes that modify the Windows graphical identification and authentication library (GINA). Moreover, desktop administration, patching and auditing tools and practices may be affected, since they cannot unlock encrypted system files without the user's credentials. If a protected system is corrupted or damaged, data recovery can be similarly affected. Finally, when routine backups are created, it's wise to encrypt those too.

Combining methods can enable an organization to obtain the best of both worlds. For example, use file/folder encryption on less capable devices like PDAs, while applying FDE to laptops. Applying both methods to the same device might seem like overkill, but it is a viable option, particularly for mobile users who carry regulated data. FDE offers foolproof protection against device loss or theft, while file/folder encryption can protect sensitive user data without obscuring files that IT requires to perform maintenance and recovery tasks.

Of course, the decision will also be influenced by workforce size and budget, privacy needs, risk tolerance and company politics.*

Lisa Phifer is vice president of consulting firm Core Competence and has written extensively about network infrastructure and security technologies.

The Ins and Outs of Database Encryption

BY RICH MOGULL

We'll look at two use cases that can help you vet your options.

There are few tasks in the practice of information security as daunting as encrypting an enterprise database. Aside from managing potential compatibility, reliability and performance requirements, security pros face a myriad of encryption options, key management pitfalls, and application integration requirements. Database encryption should never be taken lightly, but a little knowledge and planning will go a long way toward ensuring a successful project.

The first step in any encryption project is to determine what data to protect, and

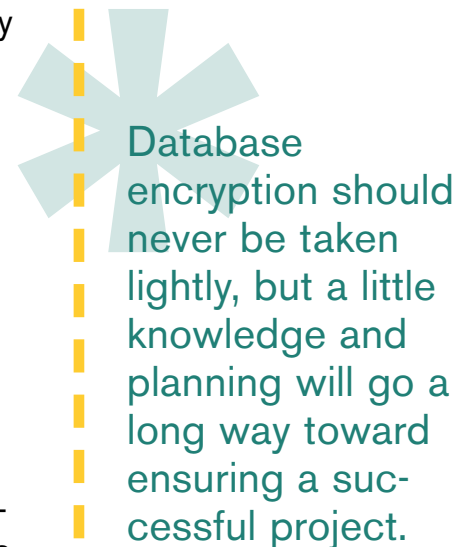
whom to protect it from. Before technology comes into play, questions must be answered, such as:

- Do you want to protect data from database users?
- Do you want to protect data from external attacks?
- Do you need to protect all the data or just a single column, like credit card numbers?

There are really only two use cases for encryption, each of which will directly determine the organization's architectural options.

ENCRYPTION FOR MEDIA PROTECTION

The first case is encryption for media protection. In this case, the entire database is likely being encrypted and the goal is to



Database encryption should never be taken lightly, but a little knowledge and planning will go a long way toward ensuring a successful project.

protect the database files or content from physical or virtual theft. The concern is that someone might steal the database files or the media they're stored on. This is the right choice if you're worried about someone hacking the server and stealing the database files, or losing them when you swap out hard drives. Although it is possible to protect the database from system administrators or other users with access to where it's stored, that won't prevent database administrators or users (or anyone who hacks their accounts) from accessing the data.

Media encryption is fairly straightforward and there are a number of good product and technology options available. Since the encryption is outside of the database, it's less likely to affect performance and won't require any database or application changes. Some database management systems include this kind of encryption as an option, allowing encryption at the table or entire database level. Alternatively, it's possible to use nearly any high-performance file- and folder-encryption tool. In both of those cases, the cryptographic operations happen on the server, and if this adversely affects performance beyond acceptable limits, consider an inline encryption appliance

with dedicated hardware to speed things up.

ENCRYPTION AND SEPARATION OF DUTIES?

The second organizational use case is encryption for separation of duties. This is the best choice if your enterprise needs to encrypt credit card numbers within a database to keep them from the eyes of administrators, and other similar circumstances. Encrypting for separation of duties is far more complex than encrypting for media protection; it involves protecting data from legitimate database users, requiring more changes to the database itself. In nearly every case, this means encrypting at the column level. If the column is an isolated field that isn't a primary or foreign key, doesn't rely on its structure for indexing performance, and isn't subject to range searches, it's a good candidate for encryption. If not, it can still be encrypted, but major database and application changes will be required.

The process of designing a new database for column encryption is a straightforward one, since you can plan as you build. Alternatively, for a complex legacy system with heavy application dependencies requiring encryption of a primary key, the project

Encrypting for separation of duties is far more complex than encrypting for media protection.

could take 2-3 years. The duration of most encryption projects falls in the middle, and the difficulty is determined by key relationships, indexing and any necessary application changes.

DATABASE ENCRYPTION RECOMMENDATIONS

All major database management systems offer column-level encryption, but none support pulling the keys out of the database by default. My recommendation is to use native encryption capabilities wherever possible, but use third-party key management products to get the keys out of the database. This strategy enables a security administrator, not the database administrator, to manage the keys to support separation of duties. Never try to encrypt a primary key. Finally, make sure you're really getting the benefits you expect—database encryption does nothing to protect against SQL injec-

tion or a compromised account with access to the field.

In terms of field encryption, avoid it on existing databases if at all possible, but to build it into new systems with sensitive data. For example, some enterprise clients are building a secure central repository with encrypted credit card numbers for transactions while pulling them out of existing systems. If there is a need for separation of duties in an existing system, consider encryption for media protection and then adding another database security technology—like database activity monitoring—for separation of duties.*

Rich Mogull has more than 17 years experience in information security, physical security, and risk management. Prior to founding independent information security consulting firm Securosis, Mogull spent seven years at Gartner Inc., most recently as a vice president.

All major database management systems offer column-level encryption, but none support pulling the keys out of the database by default.

GOLD SPONSOR

IronPort

IronPort Data Loss Prevention Resource Guide

Protect your data! Learn about Ironport's Data Loss Prevention Best Practices!

2008 Internet Trends Security Reports

Plan ahead! Understand next decade security trends before the trend comes to you.

IronPort PXE Encryption Whitepaper

Ensure that vital business information is properly secured by properly securing your data.

IronPort PXE Encryption Technology Datasheet

Revolutionary Encryption Technology: Going beyond regulatory compliance.

Email authentication Whitepaper

Understanding the authentication problem in email.

GOLD SPONSOR

Thawte

Securing your Online Data Transfer with SSL

This white paper provides an introduction to SSL security covering the basics of how it operates and how to deploy appropriate SSL certificates.

Securing your Apache Web Server with a thawte Digital Certificate

Read this white paper and learn more about securing your Apache Web Server with thawte digital certificates.

Extended Validation (EV) SSL Certificates

This white paper details the benefits of extended validation (EV) SSL certificates and how they can help your company.

Securing your Microsoft IIS Web Server with a thawte Digital Certificate

In this guide you will find out how to test, purchase, install and use a thawte Digital Certificate on your Microsoft Internet Information Services (MS IIS) web server.

The thawte Starter PKI Program

Read this white paper and learn about the advantages and benefits of the thawte Starter PKI Program.

GOLD SPONSOR

Utimaco

Download Free Trial Offer of SafeGuard Enterprise

Learn how SafeGuard Enterprise provides centralized policy based encryption for PCs.

Download Free Trial Offer of SafeGuard Easy

SafeGuard Easy provides completed data encryption for laptops and desktops—learn more.

SafeGuard Enterprise

Our flagship product for all of your data security needs—discover more here.

SafeGuard Data Exchange

This data security solution helps to secure valuable data for removable media, file encryption, email security and PDA security.

SafeGuard Configuration Protection

SILVER SPONSOR

CREDANT

Find out the Value of Unprotected Data

Download CREDANT's free Data Risk Assessment Tool.

Get the Complete Story on Encryption

Download The Next Generation of Encryption: Closing the Gap.

The Truth About Full Disk Encryption

Five questions you should ask before you buy.

Encryption Resources

Read recent articles with data security tips and solution briefs about compliance best practices.

CREDANT Mobile Guardian

The only centrally managed endpoint data protection providing intelligent encryption.

SILVER SPONSOR

Guardium

Assuring PCI-DSS Compliance with Real-Time Database Security and Monitoring

Read how database activity monitoring can protect sensitive data and satisfy PCI without impacting performance or the need to implement database encryption.

Protect Cardholder Data for PCI – Without Database Encryption

View this videocast with Guardium's CTO to learn how database activity monitoring can be used as a compensating control for database encryption (Requirement 3.4).

How Dell Simplified Database Security for SOX, PCI, SAS 70

Case study on how Dell replaced its native database logging resulting in streamlined compliance and significant reductions in auditing overhead.

10 Essential Elements for Database Security and Compliance

Learn first steps for hack-proofing your critical databases and best practices for effectively securing Oracle, SQL Server, DB2 and Sybase environments.

SILVER SPONSOR

MessageLabs

How 'DNS' Could Spell Trouble for Your Business

DNS vulnerabilities extend far beyond the world of IT reaching the heart of the business community.

MessageLabs Policy Based Encryption Service

Managed Policy Based Encryption service helps save resources at a low, predictable cost.

MessageLabs Boundary Encryption Service

Managed Boundary Encryption secures your email communications keeping with compliance.

Eliminate the Risks of Emailing Confidential Information

Read how Policy Based Encryption Service can help you secure vital business information.

How to Protect Your Email from DNS Vulnerabilities

The proper security measures can help mitigate the risks associated with DNS attacks.

SILVER SPONSOR

PGP

Five Truths About Enterprise Data Protection – The Best Way to Secure Your Data and your Business

This brochure offers insights into costs and consequences of breaches with an enterprise focus.

Nine Questions Encryption Vendors Really Don't Want to Answer

This booklet provides an easy-to-follow guide to understanding the encryption solution landscape.

The Role of PGP Endpoint in Data Protection

Protect data at the edge with security for portable data devices.

How to Deploy Comprehensive Data Protection in the Federal Government

Encryption is becoming the focus of federal government agencies as volume of information grows.

PGP Command Line Technology Overview

This Technology Overview presents examples of ways that PGP Command Line can be used to encrypt data in automated business processes.