Lock Up Your Data

SMBs Need Encryption Too!

Your data is the lifeblood of your business. Your customers trust you to keep their information secure. But what if it falls into the wrong hands? Laptops containing customer records sometimes get lost. Backup tapes disappear out of the backs of trucks. And while it may seem as if data breaches only happen to large enterprises or government entities, that's a common misconception easily explained by the fact that high-profile organizations are the most likely to receive news coverage.

If you think data breaches are not a small business problem, think again. Risk consulting firm Kroll Associates, Inc. has released its forecast for data security trends in 2011, and "more small-scale breaches" tops the list at number one.[1] "We will most likely see an increase in reported, smaller-scale breaches," the report reads. "This is not to say that the era of the massive [corporate] breach is over, but they may be matched by small-breach frequency."

By Ken Downie

Where to Start? Encryption Tips for SMBs

Any company that deals with sensitive information—from the smallest contractor to the largest enterprise—needs to encrypt that data in certain situations, either by law or to protect its own trade secrets. By encrypting confidential data, SMBs can take control of the risk that their data might be lost or stolen. The following checklist provides a roadmap for getting started with encryption.

1. Begin by thinking about your customers. Research the applicable federal and state laws that apply to encryption to protect your customers' information. At present, these regulations are most extensive for healthcare companies in the U.S.
2. Assess your company's risk profile. SMBs may wish to seek advice and guidance from outside legal counsel.
3. Educate employees about protecting confidential data. Employees will be more vigilant about practicing "safe computing;" they will be less likely to lose mobile devices and will be more careful about sending confidential data to unauthorized people.
4. Inventory locations of confidential data and delete unnecessary storage. You have to know where confidential data resides in order to protect it. Deleting this data where there is no legitimate business need for retention will instantly reduce your risk of a data breach without spending a dime.
5. Learn what security controls are required to protect confidential data. Consulting with the person who runs your network, computers, and applications will help identify requirements for security controls for protecting confidential data.
6. Put the right tools in place. SMBs with minimal technical resources should investigate product suites that combine whole disk encryption, email encryption, and encryption of files and folders to satisfy all or most of their encryption needs with a single package.

Although the aftermath of a data breach is always costly and damaging to a company's reputation, large enterprises usually have enough resources to pick up the pieces and move on. Small and medium-sized businesses (SMBs), however, can be devastated and put out of business by a single breach. To mitigate this risk, more and more SMBs are using encryption, a process that uses an algorithm called a cipher to make information unreadable. Data is encrypted using a public key, making it unreadable to anyone except those possessing the public key and a corresponding private key.

The good news is that encryption can be faster and easier to put in place than many SMBs expect.

What's driving encryption?

The drivers for encryption are multiplying, and so is its use. According to the Symantec 2010 Global SMB Information Protection Survey, 75 percent of small business owners are concerned about the possibility of a data breach.[2] They

Kurt Smith, Systems Security Officer, HealthDataInsights

> "We use whole disk encryption to ensure that if a laptop or workstation is lost or stolen, **the only damage would be the cost of the computer.**"
>
> *– Kurt Smith, Systems Security Officer, HealthDataInsights*

should be; keeping data secure means protecting the very lifeblood of business. "If you cannot securely send an email with data in it, you cannot work; you cannot create value anymore," observes Eric Domage, IDC Western Europe program manager, Security Products and Solutions. "No information sharing means no business."

But it's not just value creation and potential reputation damage driving SMBs to encrypt sensitive data. Governments are also getting into the act. In the United States, regulations such as the Health Information Technology for Economic and Clinical Health Act (HITECH) and the Payment Card Industry (PCI) Data Security Standard (DSS), as well as breach notification laws in at least 46 states, are forcing the issue in certain industries and locations (see sidebar: Encryption and Data Breach Laws in the U.S.).

Under HITECH, if any healthcare provider, even a small medical clinic, improperly discloses protected health information (PHI), the provider must notify the affected patients within 60 days of discovering the breach. If the breach involves 500 patient records or more, the healthcare provider must also notify the U.S. Department of Health and Human Services (DHHS) and the local media—not exactly a low-profile scenario. Even if a business is not a healthcare provider, it may have to comply with the U.S. Federal Trade Commission's Health Breach Notification Rule if it handles healthcare information on behalf of a customer.[3] But if sensitive data is exposed to unauthorized access and it's encrypted, regulations don't consider the incident a data breach, because it's impossible to access the data without a private key.

SMBs may also be compelled to use encryption by their customers. As more and

Encryption and Data Breach Laws in the U.S.*

Most states now have data breach laws, and expanded federal legislation is expected sooner rather than later now that HITECH has opened the door. While much of the current legislation is couched in terms such as "if reasonable and appropriate," expect laws with more teeth shortly.

Law	Who's affected?	The upshot
Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) – 2009	Companies that deal with protected health information (PHI)	HIPAA-covered entities must (if reasonable and appropriate) encrypt electronic PHI. Applies to data at rest and in transit. Breach notification requirements apply and are more severe for data breaches involving 500 or more records.
Gramm-Leach-Bliley Act (GLBA), Interagency Guidelines for Establishing Standards for Safeguarding Customer Information and FFIEC Information Security Booklet (2006)	Financial services companies	Financial institutions must adopt security measures, if appropriate, that include encryption of electronic customer information, including while in transit or in storage, on networks or systems to which unauthorized individuals may have access. Effective key management practices and endpoint encryption are also addressed.
Massachusetts General Legislature ch. 93H and 201 CMR 17.02-04	Every person that owns or licenses personal information about a resident of the Commonwealth and electronically stores or transmits such information	Mandates encryption of all transmitted records and files containing personal information that travel across public networks or are transmitted wirelessly; also mandates encryption of all personal information stored on laptops or other portable devices. Includes breach notification provisions.

Continued on next page

more organizations encrypt their data, they expect the companies they do business with to follow suit. Indeed, if your customers are encrypting, and you're working with their data, then you'll soon be encrypting and decrypting to comply with their security requirements.

At HealthDataInsights, a Las Vegas-based company that verifies the integrity of healthcare claims, encryption of protected health information is required by its customers—the Centers for Medicare and Medicaid Services, insurance companies, and government agencies such as the U.S. Department of Defense. "Even though we're a small business and not a government agency, we still need to follow the Security Technical Implementation Guides set by the Defense Information Systems Agency," explains the organization's Systems Security Officer Kurt Smith. "Because we take in PHI, our government and commercial customers require and expect us to safeguard that data from unauthorized access."

What should you encrypt? And how?

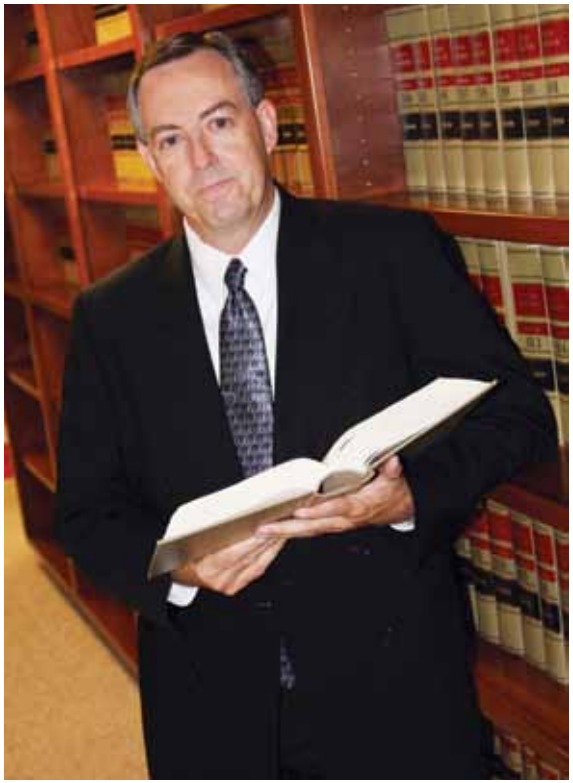
Compliance concerns often dictate what data organizations choose to encrypt first. While no federal breach notification law currently exists in the U.S., states such as Nevada and Massachusetts have introduced their own laws that go a step

Continued from previous page

Encryption and Data Breach Laws in the U.S.*

Law	Who's affected?	The upshot
Nevada Revised Statutes (2010)	Any governmental agency, institution of higher education, corporation, financial institution, retail operator, or any other type of business entity or association that, for any purpose, whether by automated collection or otherwise, handles, collects, disseminates, or otherwise deals with nonpublic personal information	Requires the use of encryption methods "adopted by an established standards-setting body" for all non-voice, non-fax electronic transmission of personal information. Includes breach notification provisions.
Nevada S.B. 227, 75th Legislature (2009)	Business accepting payment cards for goods or services in Nevada	Requires merchants to comply with the Payment Card Industry (PCI) Data Security Standard, which requires the encryption of cardholder data.

** Excerpted from **Summary of Selected Encryption Laws**, Stephen S. Wu, January 14, 2010*



Terry Bratton, Legal Administrator, Legal Aid Center of Southern Nevada

further and actually mandate encryption of certain types of data.

Doing business in Nevada? Encrypt email

In 2010, Nevada amended its existing legislation to require all entities doing business in the state to use encryption methods "adopted by an established standards-setting body" for all non-voice, non-fax electronic transmission of personal information—and that means email. Lyle Epstein, president of Kortek Solutions, a Symantec partner serving SMBs in the Las Vegas area, wanted to make sure his customers would be ready. "A lot of our clients were not aware of the new law, so we let them know we were able to provide a solution for them," he says.

> "PGP **provided us with a very quick answer** in response to Nevada's amended encryption law."
>
> *– Terry Bratton, Legal Administrator, Legal Aid Center of Southern Nevada*

One of Kortek's customers is Legal Aid Center of Southern Nevada, a full-service law firm that has provided free legal aid to Clark County's low-income residents since 1958. Because the organization frequently sends emails containing sensitive personal information, it wanted to encrypt those emails to comply with the new Nevada statutes. "One of our requirements was that we didn't want the emails sent to a third party for encryption," says Terry Bratton, legal administrator. "We wanted to retain the messages at all times."

Kortek recommended implementing PGP Universal Gateway Email running on PGP Universal Server from Symantec to provide centrally managed, standards-based encryption without sending the emails off site. "PGP Universal Gateway Email is very well suited to the SMB market," explains Epstein. "When we looked at other competitive products, not only were they more geared toward the enterprise, but they weren't priced within reach of the small and medium business community. It's also very easy to deploy."

Now, when users send an email containing personal information about a client, they can either click a toolbar button or type the word "confidential"

MICHAEL BRUNETTO

Lyle Epstein, President, Kortek Solutions

into the subject line, instructing PGP to encrypt the entire message, including any attachments. By encrypting data at the gateway, PGP Universal Gateway Email ensures data is protected from unauthorized access in transit and at rest on a recipient's mail server. Email is delivered encrypted regardless of the recipient's use of encryption, and recipients do not need to install any software to read encrypted messages.

"PGP has been working very well," says Bratton. "The rollout was very easy, and our staff adapted to it quickly. It provided us with a very quick answer in response to Nevada's amended encryption law."

Handling protected health information? Encrypt whole disks and file shares

HealthDataInsights must encrypt more than just email to comply with its customers' requirements. The company uses PGP Whole Disk Encryption and PGP NetShare, along with PGP Universal Server, to encrypt whole disks, backups, and data streams, as well as loose files and folders.

"We use whole disk encryption to ensure that if a laptop or workstation is lost or stolen, the only damage would be the cost of the computer, because none of the data on the hard drive is readable," says Smith. "We have policies stating that people aren't supposed to have any kind of sensitive data on their personal computer, but we didn't want to take people's word for it, because people make mistakes. Almost all of our customers use PGP and are happy with it, so it was the logical choice for us. PGP is even ahead of governmental requirements."

Webcast
Improving Data Protection with Symantec Endpoint Encryption.

For network file and folder encryption, PGP NetShare enables HealthDataInsights to create files that can be stored anywhere on the network, backed up, and moved as needed, but unlocked only by team members who have the proper keys. "PGP NetShare is one of the coolest features, especially when it comes to documents and contracts," Smith explains. "Simply applying folder- and share-level security is inadequate, because high-level administrators still have physical access to all the data. With PGP NetShare, administrators are able to restore files or move them around, but they do not have access to read

MICHAEL BRUNETTO

the data unless they're part of the right security group."

Will encryption be disruptive?

While having the right encryption tools in place is important, having the right key management tool is absolutely essential. Keys and encryption policies need to be managed centrally, notes IDC's Domage. "Organizations using encryption need a centralized repository for key management, whether the encryption technology is coming from vendor A, B, or C," he says. "Businesses don't want to be in a position where they lose an employee, lose a key, and therefore lose access to critical data."

PGP Universal Gateway Email offers central management of encryption keys, helping Legal Aid Center of Southern Nevada minimize user confusion and disruption. "It's actually very easy to use," says Bratton. "One of the other things that we like about not going through a third-party provider is that we're able to monitor the keys ourselves and report on exactly what the user access has been." Currently, penalties for noncompliance with the Nevada law are unclear, but "we want to make sure that we have the ability to show that we are, in fact, compliant," he says.

By using a single, unified console such as PGP Universal Server, SMBs can easily manage multiple encryption applications and enforce security policies automatically. "Encryption is becoming ubiquitous—it's in the Microsoft Windows operating system, smartphones, e-commerce—but few organizations are managing it centrally," says IDC's Domage. "Without a centralized policy, encryption can turn into chaos, and companies have no way of enforcing its use."

> "Organizations using encryption **need a centralized repository** for key management."
>
> *– Eric Domage, Western Europe Program Manager, Security Products and Solutions, IDC*

COMPANY PROFILES

HealthDataInsights

Founded: 2004
Location: Las Vegas, Nevada
Website: *www.healthdatainsights.com*
Employees: 300
Business Activity: Verifies integrity of healthcare claims and billing
Encryption Technologies Used: PGP Whole Disk Encryption, PGP NetShare, PGP Universal Server

Legal Aid Center of Southern Nevada

Founded: 1958
Location: Las Vegas, Nevada
Website: *www.lacsn.org*
Employees: 60
Business Activity: Provides legal services to low-income residents
Symantec Partner: Kortek Solutions (*www.korteksolutions.com*)
Encryption Technologies Used: PGP Universal Gateway Email, PGP Universal Server

HealthDataInsights runs PGP Universal Server in Guarded Key Mode, which stores a passphrase-protected copy of end users' private keys on the PGP Universal Server. "Users don't have to worry about backing up their keys, because Universal Server has taken care of that for them," says Smith. "And if someone's system dies, their keys are available on their rebuilt computer. As for public keys sent to us by our customers, we store them in our password database, but we don't really worry about it too much."

Smith continues: "One of the advantages of using the same encryption technology as our customers is that PGP Universal Server automatically takes every user's public key and places it up on PGP's Web-accessible directory. So when we need to transfer that data, we don't need to have to send the customer our public key—they can just find it on the Internet, which makes it very straightforward. I can't think of a better way to manage encryption keys.

Where's the ROI?

Encryption can pay for itself very quickly by mitigating the risk of data breaches and demonstrating to customers and regulators that data is protected. In more and more cases, SMBs must encrypt to mitigate risks that could put them out of business.

Says HealthDataInsights' Smith: "PGP paid for itself within the first month of deployment. We were able to use it as a sales tool and put our customers at ease. We've used other encryption technologies in the past, but PGP has been the simplest and most effective solution. It's an integral part of how we safeguard our data." ■

[1] Brian Lapidus, 2011 Data Security Forecast: Top Ten Trends for the Year Ahead, Kroll Associates Inc., December 2010.

[2] 2010 SMB Information Protection Survey Global Data, Symantec Corporation, June 2010.

[3] Federal Trade Commission, 16 CFR Part 318 Health Breach Notification Rule; Final Rule, Federal Register, Vol. 74, No. 163, August 2009.

Ken Downie is a Senior Writer at NAVAJO Company. His work has appeared in Business Finance, Business Credit, *and* CIO Digest *magazines.*

Symantec Encryption Options

Endpoint Data Protection
- Symantec Endpoint Encryption
- PGP Endpoint Device Control
- PGP Whole Disk Encryption
- GuardianEdge Device Control
- GuardianEdge Encrypted Drive Manager
- GuardianEdge Hard Disk Encryption
- GuardianEdge Removable Storage Encryption

File and Server Protection
- PGP Command Line
- PGP NetShare

Email and Mobile Protection
- MessageLabs Hosted Email Encryption
- PGP Desktop Email
- PGP Mobile
- PGP Support Package for BlackBerry
- PGP Universal Gateway Email

Management
- PGP Key Management Server
- PGP Universal Server
- GuardianEdge Advanced Authentication
- GuardianEdge Altiris Connector
- Symantec Data Loss Prevention

Product Packages
- PGP Desktop Professional
- PGP Desktop Storage

Symantec.