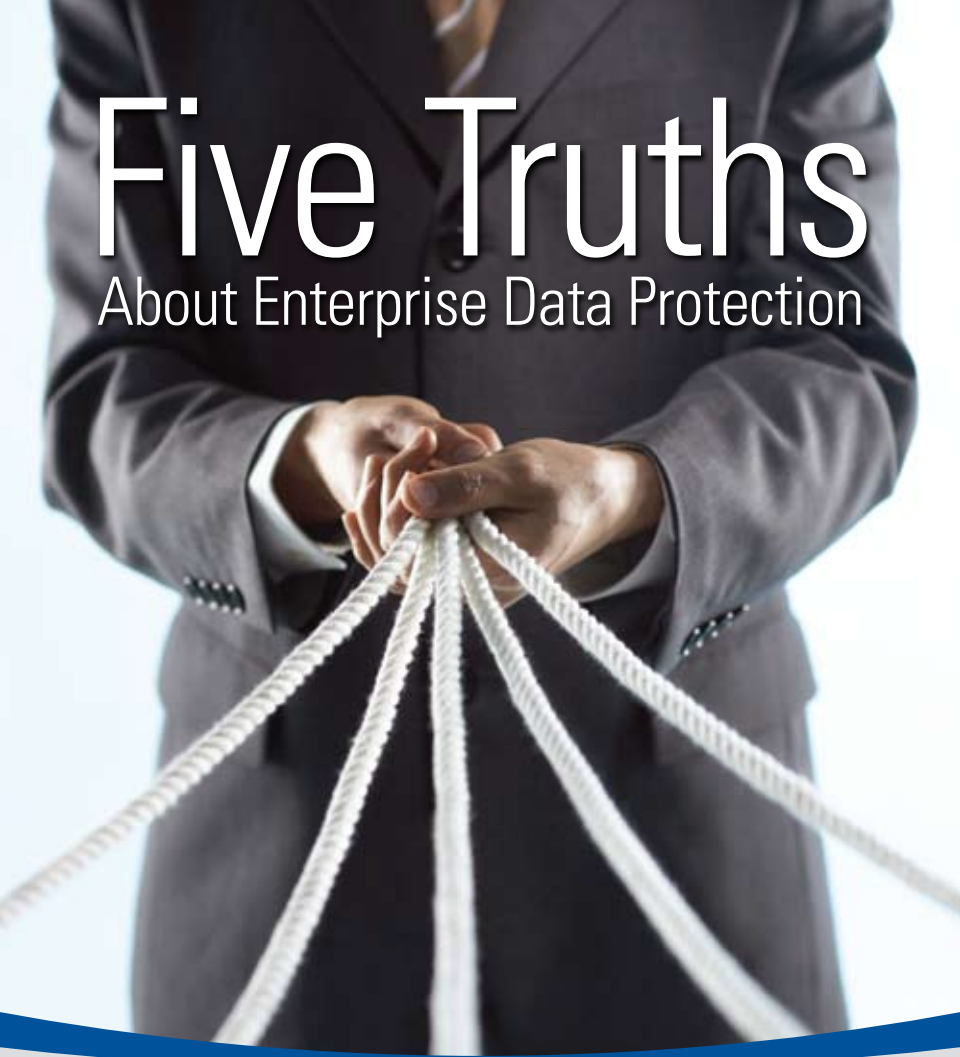


Five Truths

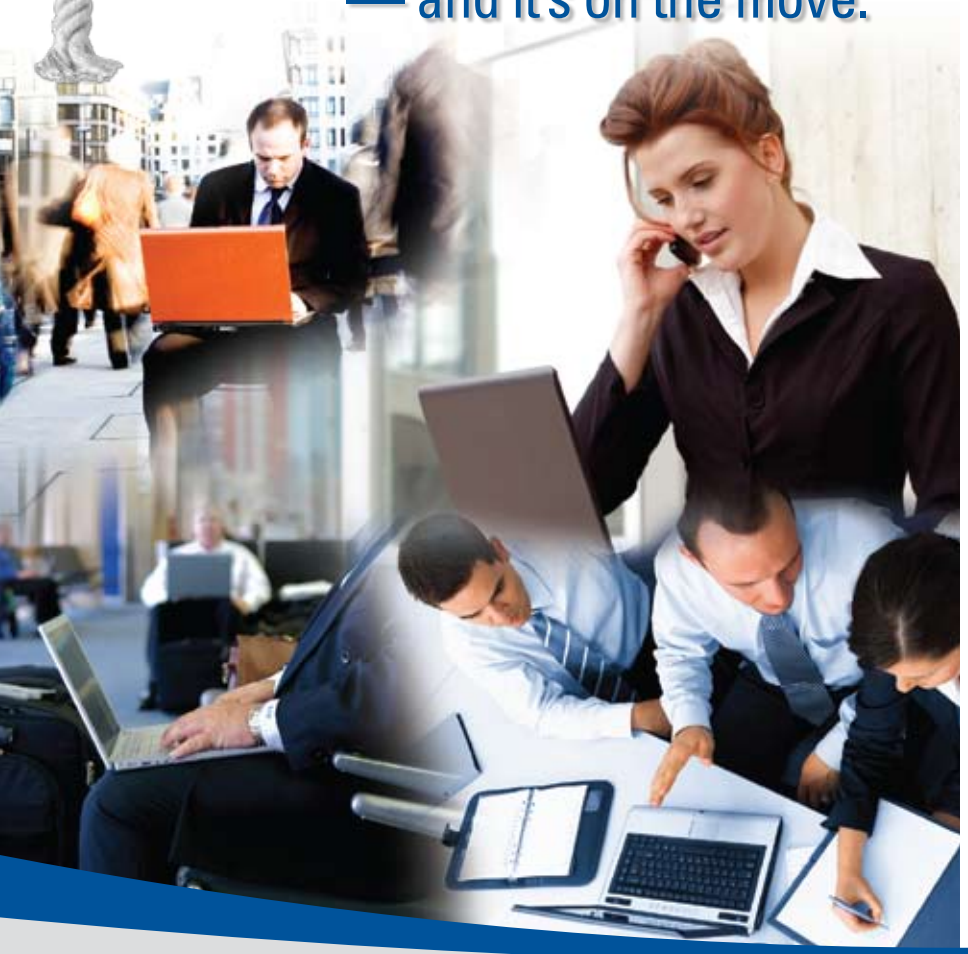
About Enterprise Data Protection

THE BEST WAY TO SECURE YOUR DATA — AND YOUR BUSINESS

PGP®

DEFENDING THE DATA

1. Business data is everywhere — and it's on the move.



Data has always played a vital role in business. Today, automated business processes and services are driven by essential data that is more mobile than ever before. The accelerating pace of business means that data is transferred faster, stored on more devices, and shared more often — with more people, around the world.

As a result, your business data is increasingly vulnerable. In fact, a recent survey by The Ponemon Institute® found that 84% of corporate organizations had suffered at least one data breach in the previous year, and 57% had experienced two or more.[1]

The reason for the increased risk of data breaches: data is now more mobile. Laptops, USB flash drives, and mobile phones routinely carry data out of the office. Emails transmit sensitive business information throughout the day. Data stored on file servers is accessed and shared across offices and business units. And outsourcing is more common, placing more confidential information in the hands of third parties.

How can your business secure data that is always on the move?

Protecting laptop and desktop computers is just the beginning. Only going to the source — protecting the data itself, no matter where it is stored or how it is transferred — lets organizations secure all their information, and their business. Even securing every email and strengthening firewalls is not enough.

2. Exposed data carries high costs & consequences.

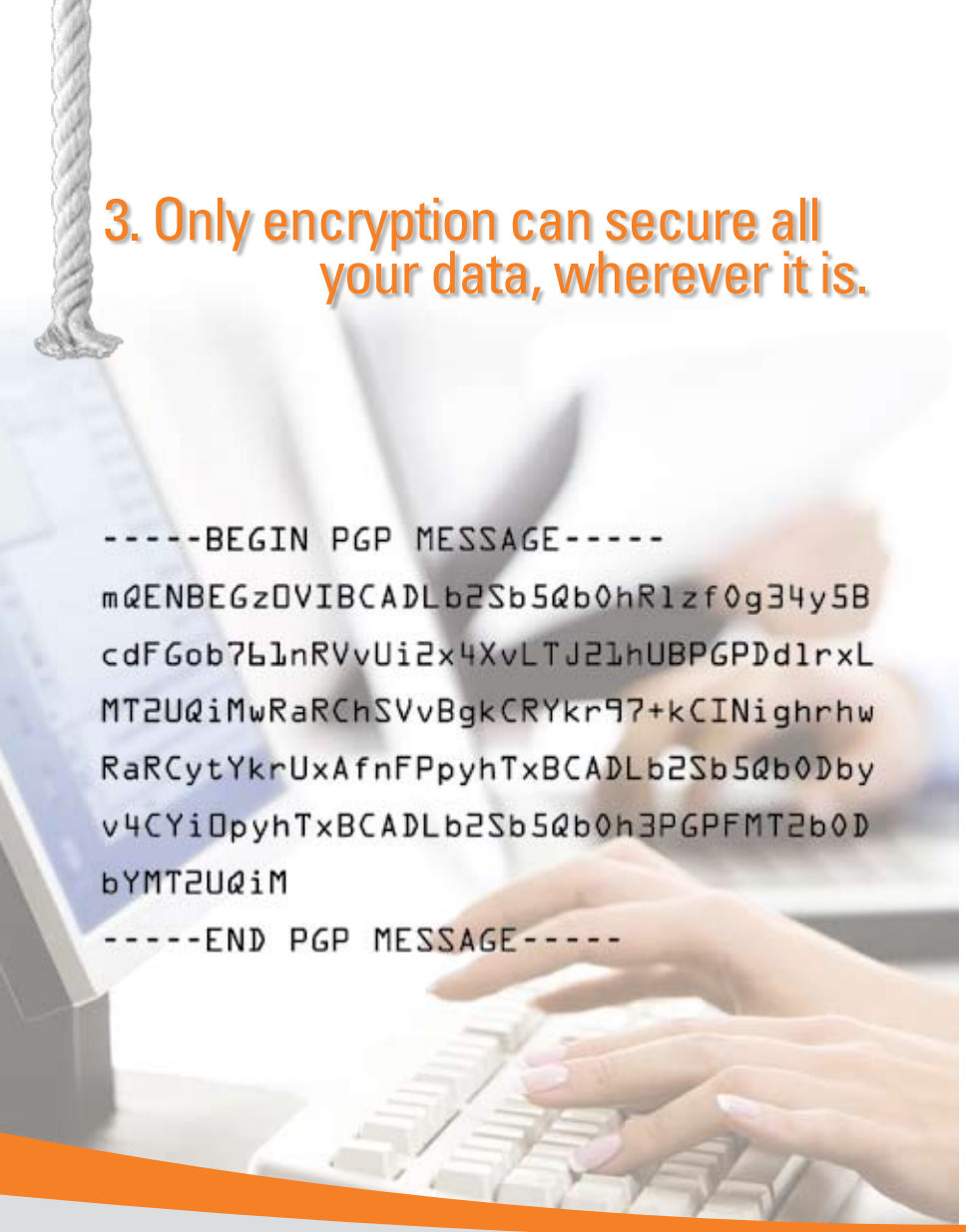
Data breaches not only affect your bottom line, they could put you out of business. For some enterprises, there is simply no way to recover from the average $6.3 million[2] cost of a data breach, and the public embarrassment and customer dissatisfaction resulting from brand damage that accompanies it.

Between 2005 and 2007, the cost of data breaches rose 43%, and the per-record cost is now $197.[3] Most of this cost is lost business: churn and the added costs to acquire new customers. The other costs include fines imposed by regulators and opportunity costs incurred from the loss of intellectual property.

The growth of outsourcing also contributes to the increased costs of data breaches. In 2005, third-party data breaches cost $12 more per-record than internal data breaches. In 2007, that difference grew to $67, increasing more than 450 % since 2005.[4]

Perhaps the most important consequence of data breaches is that they undermine your brand and the business name that you have built for years. Research shows that customers have not grown accustomed to data breaches.[5] They rightly assume that their information — and all the data housed within your business and transferred in and out of it — should be protected from hackers, thieves, and accidental loss.

3. Only encryption can secure all your data, wherever it is.



During a business day, a single file could be emailed, stored on a file server, carried out of the office on a laptop, and transmitted over a smartphone. No firewall, single agent, or security point solution is able to protect a file wherever it goes.

That is why encryption is increasingly recognized by leading IT organizations as the business standard for enterprise data protection.

Only encryption protects the data itself. Encryption turns a sensitive information file into a cryptographically secure file that can be read only by designated parties. That means the data can be stored safely, transmitted safely, and carried out of the office on any type of device.

With data encryption, wherever your business data goes, its protection is built in.

4. An enterprise-wide data encryption strategy reduces the risk of data breaches.

You can use encryption to protect your business data at rest, and on the move. In fact, your organization can adopt an always-on, strategic approach to securing all its data.

Organizations that implement an enterprise data encryption strategy reduce operational expenses, can add encryption applications as needed, and eliminate redundant IT administrator tasks.

Instead of following the silo approach of acquiring, deploying, and managing multiple and disparate encryption solutions, the organization can deploy a single enterprise-wide data encryption platform. The platform approach enables the organization to centrally manage and deploy multiple encryption applications — such as email, laptop, or backup tape encryption — with consistent and centralized policy enforcement, including key management.

Research shows that organizations that implement an enterprise-wide encryption strategy significantly reduce the risk of a data breach. Organizations with partial encryption strategies (encrypting only certain data applications) and organizations with no strategy are far more likely to have suffered one or more data breaches in the past year.[6]

Research also shows that organizations that use the holistic approach of an enterprise encryption strategy are less likely to incur the costs and brand damage associated with data breaches and are likely to have a more profitable business.[7]

5. Enterprise data protection liberates your business.

An enterprise-wide encryption platform is the foundation of enterprise data protection. What is enterprise data protection? It is a comprehensive, strong security system, comprising four components, that enables a business to protect all of its data, all of the time, wherever it is stored and however it travels:

- **Protect data:** Use standards-based encryption to protect the data itself, whether at rest or on the move.
- **Detect risk:** Identify security risks and develop strategies to mitigate exposure, enforce policies, and prevent data leakage.
- **Control access:** Use authentication — including hardware tokens, smart cards, and identity management — to control access to data.
- **Manage data:** Centrally manage and deploy multiple encryption applications and keep data accessible throughout its lifecycle — including in storage, backup, and archive — so that business continues uninterrupted.

An encryption platform approach makes this all work together by providing key management across applications, offering a centralized administrative interface, and automating policy enforcement. It is easy to use, simple to deploy, improves productivity, and reduces security expenses.

With enterprise data protection, your salespeople, accountants, customers, contractors — anyone who works with sensitive, private, or proprietary information — can focus on communication, collaboration, and innovation. And you can focus on liberating, not defending, your business.

The PGP® Encryption Platform Difference

The PGP Encryption Platform reduces the complexities of protecting business data by enabling organizations to deploy and manage multiple encryption applications cost-effectively from a single management console. Most importantly, the PGP Encryption Platform provides the automated services, centralized management, consistent policy enforcement, and extensible framework needed to develop and deliver a comprehensive, lasting enterprise data protection strategy. **www.pgp.com**

[1]The Ponemon Institute, *2008 Annual Study: U.S. Enterprise Encryption Trends*, p. 11.

[2]The Ponemon Institute, *2007 Annual Study: U.S. Cost of a Data Breach*, p. 2.

[3]Ibid., p. 2.

[4]Ibid., p. 12.

[5]Ibid., p. 7.

[6]The Ponemon Institute, *2008 Annual Study: U.S. Enterprise Encryption Trends*, p. 12.

[7]Ibid., p. 12.

PGP®

DEFENDING THE DATA

PGP Corporate Headquarters
200 Jefferson Drive
Menlo Park, CA 94025
U.S.A.
Tel: +1 650 319 9000

PGP (GB) Ltd.
Tel: +44 (0)20 8606 6000

PGP Deutschland AG
Tel: +49 69 838310 0

PGP Japan K.K.
Tel: +81 03 4360 8308