2008 Annual Study:
U.S. Enterprise Encryption Trends

Leading IT organizations continue shift to strategic encryption approach

A study analyzing survey results from 975 U.S. business and IT managers about their current and future needs, motivations, uses, budgets, and strategies for enterprise data protection.

March 2008

Research conducted by

Ponemon Institute, LLC

The information in this document is provided “as is” without warranty of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement.

This document could include technical inaccuracies or typographical errors.

Changes to this document may be made at any time without notice.

Table of Contents

Executive Summary

In this decade, a new rule is now part of operating any business: Failure to protect customer data and proprietary business information can lead to serious consequences. The loss of customers, difficulty acquiring new ones, irreparable brand damage, and even industry fines are now all part of failing to live up to the business commitment of protecting data. For the third year, research by The Ponemon Institute revealed the average cost of a data breach continued to rise, growing 43% since 2005 to an average $197 per record compromised. With a very real impact, data breaches cost an average of $6.3 million.[1]

To defend customer data and eliminate the potential consequences of a breach, businesses are encrypting sensitive data. For organizations impacted by a data breach, increasing the use of encryption is the most often technology used to prevent another breach from occurring.[2] As part of lessons learned, tactical threat evaluation, or an overall enterprise data protection strategy, organizations are expanding their use of encryption across the enterprise and beyond.

This 2008 study by The Ponemon Institute, sponsored by PGP Corporation, focuses on identifying trends in encryption use, planning strategies, budgeting, and deployment methodologies in enterprise IT. 975 U.S.-based IT and business managers, analysts, and executives participated in this second annual survey. Nine percent of respondents were at the vice president level or higher, and 38 percent were at the director level or above.

With the rising cost of data breaches an accepted business reality and the need for encryption more apparent than ever, the study sought to answer questions about the use of and strategy for enterprise encryption: Why are enterprises using encryption? What encryption applications are in use? How are organizations planning for encryption? Can the adoption of an encryption strategy reduce the risk of a data breach? How are organizations budgeting for encryption? How much are organizations spending on key management? What type of encryption approach do they prefer? Are leading IT organizations adopting a strategic approach to encryption, as might be expected?

To understand how organizations are performing and identify IT leaders, The Ponemon Institute continues to track the index of an organization's IT security effectiveness known as the Security Effectiveness Score (SES). The SES is based on respondents' self-evaluation of their IT organization across 24 attributes and is used throughout the study to answer questions, make comparisons, and identify trends.

Key Findings

- **Strategic encryption planning grows.** In response to increasing demands for enterprise data protection, more organizations are planning strategically for their encryption needs. 21 percents of organizations surveyed now have an encryption strategy applied consistently across the organization, up from 16 percent in 2007. 74 percent organizations have some type of encryption strategy either enterprise-wide or applied based on the type of data or applications used. As expected, leading IT organizations with the most effective security programs (high SESs) are the ones at the forefront of this strategic planning trend and continued to improve the effectiveness of their IT organizations in 2008.

- New: **Data breaches occurring often but encryption strategy makes a difference, prevents data breaches.** 84 percent of organizations surveyed suffered at least one data breach over the

[1] The Ponemon Institute, "2007 Annual Study: Cost of a Data Breach", November 2007
[2] Ibid.

last 12 months. In fact, 44 percent of organizations suffered two to five breaches during the past year. However, organizations with an enterprise encryption strategy showed a statistically significant lower rate of data breaches. This demonstrates that an encryption strategy, especially one implemented across the enterprise, reduces the costs and brand damage associated with data breaches and likely leads to a more profitable business.

- **Encryption use across multiple applications growing.** Respondents reported the consistent encryption of laptops, emails, and backup tapes increased. Laptop encryption is the most common, with 20 percent reporting use most of the time. The use of encryption is driven now more than ever by the need to mitigate the consequences of a potential data breach: 71 percent rated this as the top reason for deploying encryption, up from 66 percent in 2007.

- **New: Key management budgeted for in 2008, organizations seeking to reduce operational costs.** Organizations surveyed on average plan to spend 34 percent of their total encryption budget on key management solutions. Key management involves the active management of encryption key lifecycle, policy, and reporting. 45 percent of organizations expect their key management investments to reduce the overall operational costs of enterprise data protection. Only 6 percent of organizations expect key management to increase the operational costs of enterprise data protection.

- **New: Single enterprise vendor for key management preferred.** Already in 2008 organizations are looking to select a single enterprise vendor for their key management needs. 58 percent of organizations expect to deploy a single enterprise-wide key management solution or deploy a single vendor's key management solution for different purposes in 2008. Only 13 percent of organizations are seeking a tactical key management solution for one encryption application.

- **Organizations more interested in a platform approach.** With a need to enforce policy and increase automation for key management, respondents were overwhelmingly interested in a platform approach, with up to 75 percent rating key features as important or very important. As described in the survey, a platform enables an organization to centrally manage and deploy multiple encryption applications with consistent policy enforcement including key management. Respondents from the most effective security organizations were much more interested in a platform strategy than those from ineffective organizations.

- **Platform approach seen as reducing costs and improving efficiencies.** Respondents believe an encryption platform approach enables their business to reduce expenses and improve productivity. They identified the top three benefits of this approach:

    - Reduction of operational expenses (63 percent of respondents)
    - Flexibility to add other encryption applications in the future, as needs (61 percent)
    - Eliminates redundant administrator tasks (54 percent)

Conclusion

IT organizations continue to overwhelmingly look to adopt a strategic platform approach. Instead of being forced to address inconsistencies across the enterprise, they want to centrally manage and deploy all encryption applications with consistent policy enforcement. The widespread use of encryption—from laptops to file servers—has already prompted many organizations to begin planning strategically. And those with the most effective IT operations are leading the way. This is not only a best practice but is now shown to materially reduce the rate of data breaches.

To achieve the broad use of encryption, and in turn lower the risk of a data breach, IT leaders believe strongly the platform approach to encryption is the most effective means compared to adopting individual point applications. The platform solution appears to be the next step in the evolution of encryption and the majority of organizations will spend their key management budgets adopting an encryption platform approach in 2008.

Introduction

In just a few years, the reality of data breaches and their consequences have become all too well known. If a security breach occurs, the risks are plentiful: damage to brand equity, the burdensome costs of notifying affected customers, possible exposure of intellectual property, and failure to comply with government regulations.

These outcomes can have significant financial consequences. For the third year, The Ponemon Institute examined the costs incurred by companies after experiencing a data breach. The research showed that the average total cost—including notification costs, loss of customers, and increased difficulty in acquiring new customers—was $6.3 million per breach.[3] The hundreds of data breach incidents reported during the past few years[4] have increased awareness of these security risks, prompting organizations to act.

IT organizations are constantly challenged by the need to secure data. Data is everywhere and no longer confined to the relative safety of the enterprise network. Business is becoming more mobile, more closely integrated with business partners, and more dependent on business process outsourcing. Instead of attempting to add more network barriers or lock data behind the firewall, IT security is shifting to build data security in – protecting data wherever it goes. This approach to enterprise data protection requires the broad deployment of encryption to secure data through the enterprise and beyond.

Until recently, a silo approach was the only option for adding encryption to the enterprise. For each type of data security required, a company had to acquire, deploy, and manage a separate encryption product. This approach does safeguard data, but at a cost: Businesses are bogged down by redundant tasks, unable to manage all encryption applications from one central console, challenged with retaining access to corporate data with an increasing number of encryption keys, and incapable of quickly expanding their security strategy to accommodate the steady stream of new productivity applications.

This is not a new situation for IT organizations. The same problem existed during the evolution of enterprise resource planning (ERP) and customer relationship management (CRM) software. Both required multiple applications—each with separate deployment and management—until IT organizations adopted a platform approach that centralized management, reduced redundant tasks, and allowed them to add new applications quickly and easily.

Now, the same approach is available for encryption, referred to as an encryption platform, raising the question: Where do IT organizations stand with their encryption implementations, how are they budgeting for encryption, are they interested in an encryption platform approach, and does taking a more strategic approach to encryption reduce the risk of data breaches?

[3] Ibid

[4] The Privacy Rights Clearinghouse, http://www.privacyrights.org/ar/ChronDataBreaches.htm

Study Overview & Methodology

The purpose of this study by The Ponemon Institute is to identify trends in encryption planning, deployment preferences, and spending among U.S. IT organizations. The study surveyed 975 U.S.-based IT and business managers, analysts, and executives employed in corporate IT departments. The questions focused on how they plan and manage encryption at their companies, whether or not they feel their organizations' security efforts are effective, and their interest in new deployment frameworks and methodologies.

The randomly selected sample was built from lists of information security professionals. In total, 13,448 subjects were invited to participate in the survey, resulting in 975 usable responses. Only surveys that passed reliability tests were used in the final sample. This final sample represents a 7.3 percent net response rate.

Data was captured through a secure extranet site, and The Ponemon Institute paid respondents nominal compensation for their time. The margin of error on all adjective or ordinal responses is ≤ 3 percent for all completed items.

Following are demographics and organizational characteristics for respondents. Table 1 provides the self-reported organizational level of respondents. The majority of sample respondents are at the manager (31 percent) or director (29 percent) levels, respectively.

Position	Percentage
Senior Executive	2%
Vice President	7%
Director	29%
Manager	31%
Associate/Staff	27%
Other	3%

Table 1: Study participants by position

On average, respondents have 11 years of experience in the information security field, and 5 years' experience in their current position. In total, 76 percent of respondents are male and 24 percent are female. Although results are skewed on the gender variable (more male than female respondents), this situation is consistent with known demographics about the information security industry within the United States.

Table 2 reports the distribution of respondents by major industry classification.

Industry (Top 10)		Percentage
1.	Financial Services	20%
2.	Government	17%
3.	Technology & Software	12%
4.	Health Care	9%
5.	Manufacturing	9%
6.	Telecom & Cable	8%
7.	Hospitality	5%
8.	Transportation	4%
9.	Retailing	4%
10.	Professional Services	4%

Table 2: Top 10 respondent industry classifications

Key Report Findings

Strategic encryption planning grows. Organizations continue to take a more proactive approach to enterprise data protection and continue to increase the strategic planning for encryption. These plans range from company-wide policies that are consistently applied throughout the organization to plans that cover only specific areas of the company's data.

Figure 1 shows that 21 percent of organizations now plan and implement an encryption strategy across the enterprise, up from 16 percent in 2007. The majority of organizations, 74 percent, have some type of encryption strategy. This is up from 66 percent in 2007 as the percentage of organizations without some form of encryption strategy declined from 34 to 26 percent.

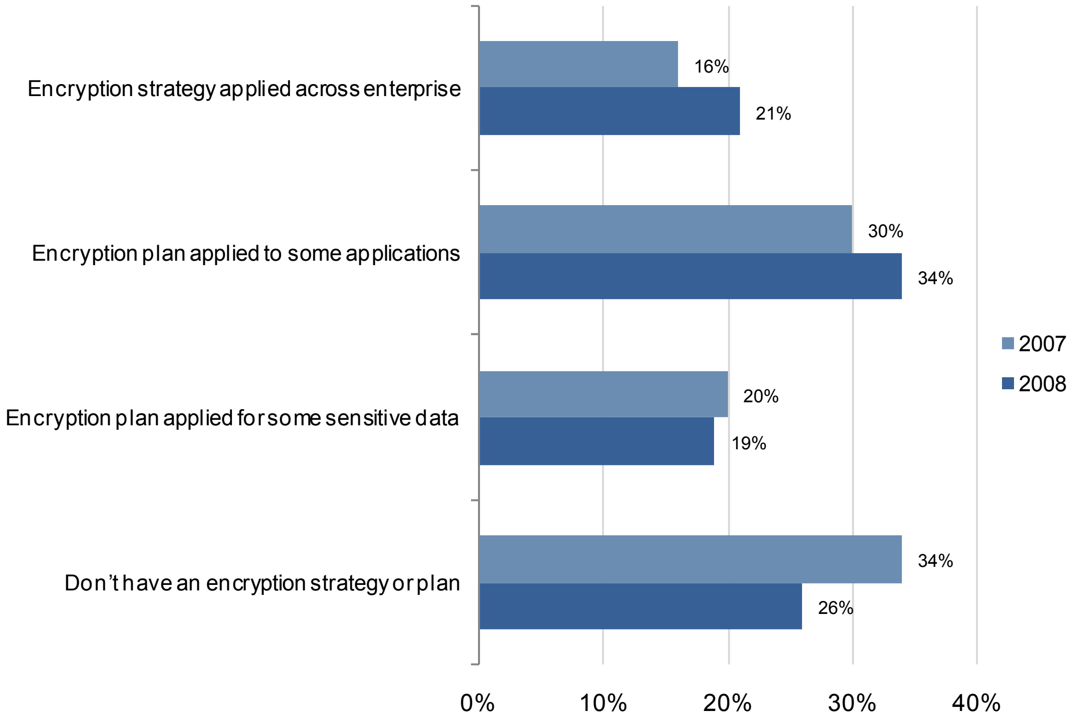

Figure 1: Encryption strategy and implementation

Leading IT organizations plan strategically for encryption. For the second year, further analysis shows that the organizations with the most effective security programs (highest SES) have taken a strategic approach to encryption. For 2008, organizations that are implementing an enterprise-wide encryption strategy increased the overall effectiveness of their IT security programs. These organizations are at the forefront of leading the IT security industry. As Figure 2 on page 9 illustrates, companies with ineffective security programs continue to not plan strategically for encryption.

Security Effectiveness Scores (SESs) reflect the confidence levels of IT security practitioners with respect to their organization's overall security and internal controls. Scores are based on the average of individual responses made to 24 attributes considered critical to the success of IT security. (The list of these attributes can be found in the Appendix, beginning on page 14.) The highest-possible SES for a respondent's organization is +2 and the lowest is -2.

For 2008 the average SES increased to 0.703 from 0.667 in 2007. Overall, respondents feel their IT security programs improved since 2007.

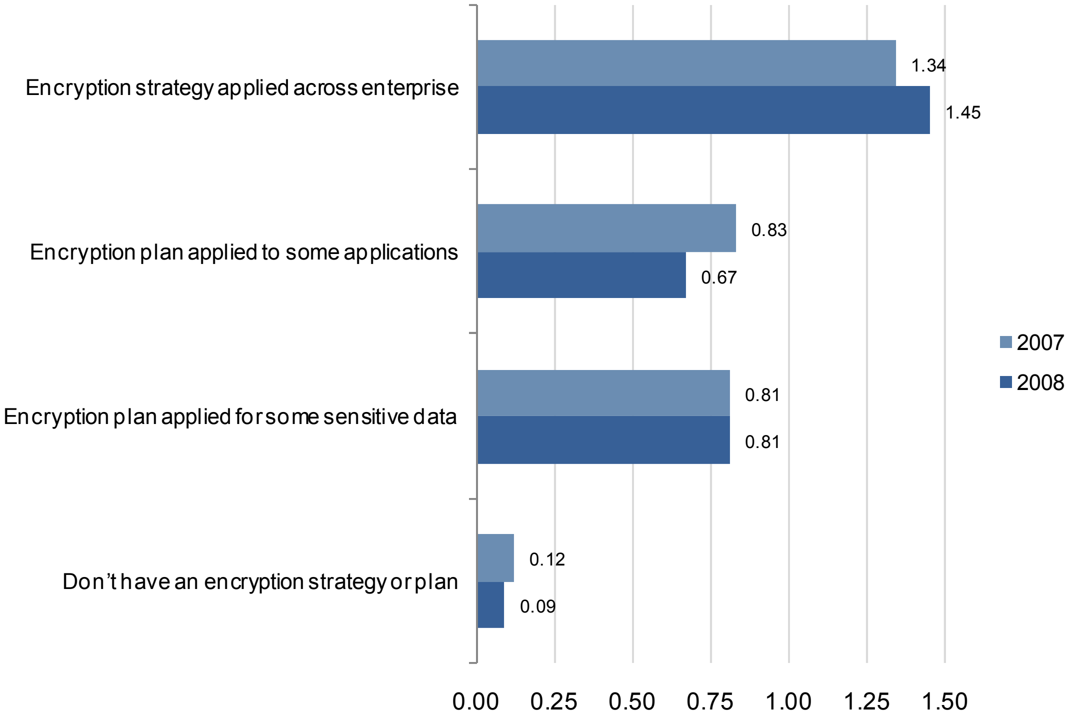

Figure 2: IT leaders (high SESs) plan more strategically for encryption use

Why companies use encryption. Figure 3 on page 10 shows that mitigating data breaches, complying with privacy or data security regulations, and protecting their company's brand remain the top three reasons why organizations use encryption. It is not surprising that mitigating data breaches continue to be the leading reason for encryption use. A data breach has a cascading effect and can lead to multiple consequences—from the exposure of intellectual property to the loss of customers.

Between 2005 and 2007, the financial toll data breaches took on businesses increased dramatically. According to The Ponemon Institute's 2007 study, the average cost of a breach per customer record increased by 43 percent compared to 2005.[5] Lost business due to higher churn rates and lower new customer acquisition increased by 71 over the three years.

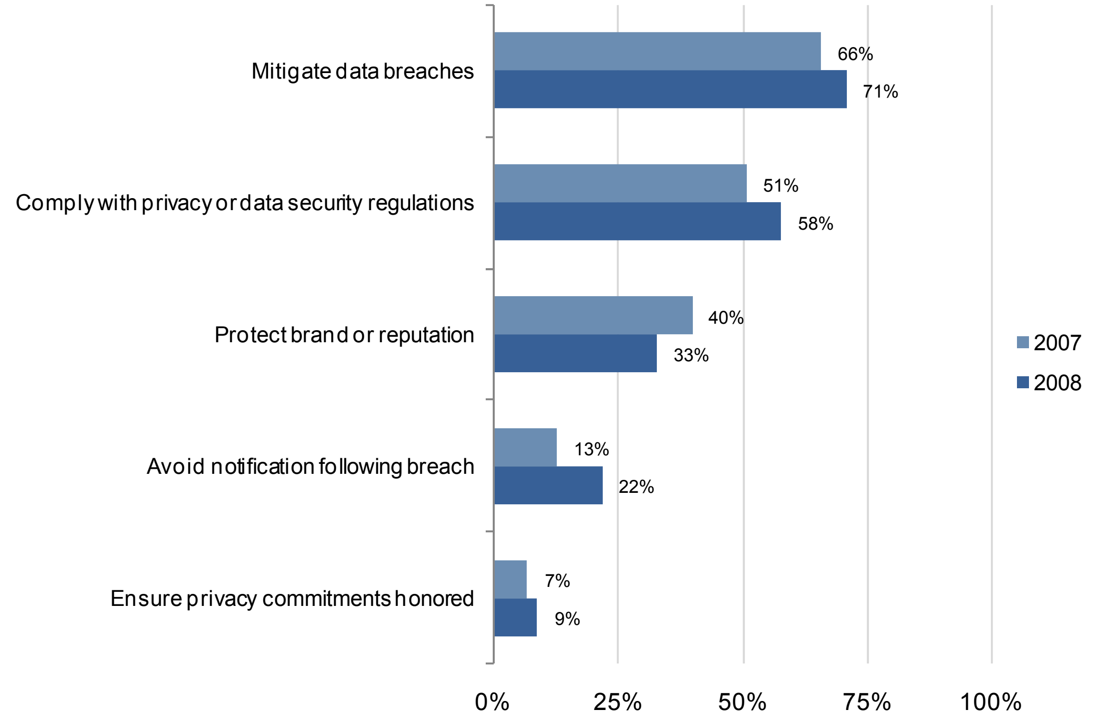

Figure 3: Top reasons why organizations encrypt sensitive/confidential data

[5] The Ponemon Institute, “Lost Customer Information: What Does a Data Breach Cost Companies?”, November 2005

Data breaches occurring often but encryption strategy makes a difference, prevents data breaches. Does an enterprise encryption strategy make a difference? Over the past 12 months, 84 percent of organizations surveyed suffered at least one data breach. The majority of organizations (57 percent) suffered two or more data breaches in the past year as shown in Figure 4.

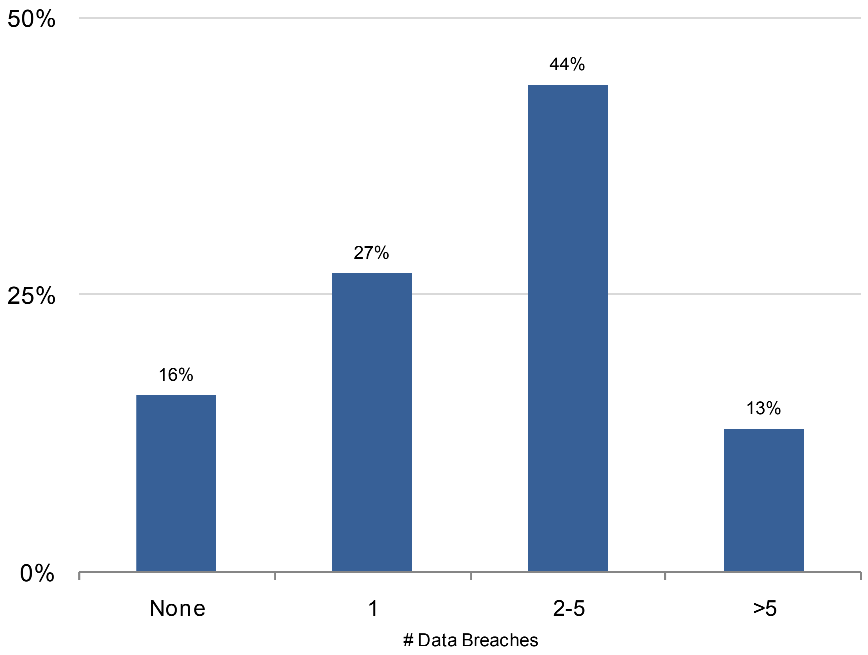

Figure 4: Number of data breaches over the last 12 months

Respondents reporting the number of breaches that occurred in their organizations

Figure 5 on page 12 shows that as the ratio of enterprise encryption strategy vs. partial strategy vs. no strategy increases, there is a statistically significant reduction in data breaches. Chi-square statistical analysis shows that the trend in data breaches is significant at $p<0.01$. Therefore, the implementation of an enterprise-wide encryption strategy does reduce the risk of a data breach. Organizations with an encryption strategy are less likely to incur the financial impact of a data breach and are likely more profitable.[6]

[6] Overall corporate performance and industry operating margins considered equal for the purpose of analysis.

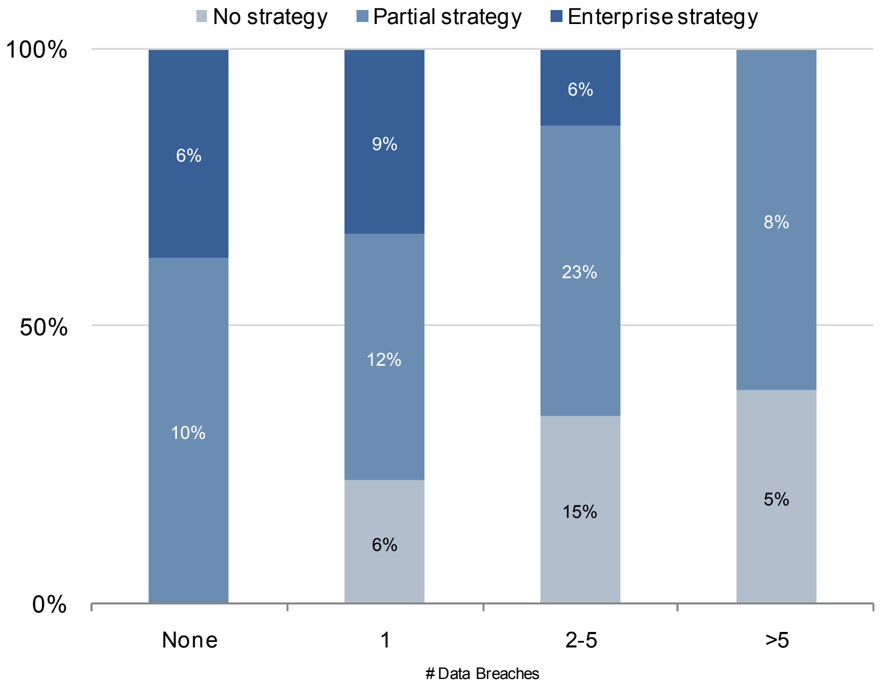

Figure 5: Comparison of encryption strategy approaches and data breaches over the last 12 months

Ratio of enterprise-wide encryption strategy to other approaches is highest for no data breaches

Companies are using more encryption applications. Figure 6 on page 13 shows the percentage of respondents reporting consistent encryption use in various application categories. Also included are numbers from a 2005 study by The Ponemon Institute.[7] As illustrated, all areas increased from 2006 to 2007 except file server encryption. While mobile data protection (e.g. laptop encryption) is the most common encryption used consistently, tape backup encryption saw the greatest percentage increase from 2006 to 2007.

The increasing use of encryption can put a strain on IT organizations that have taken a silo approach. As they add encryption applications to address new technologies, they must undertake more repetitive tasks, shoulder higher operational costs, and support a more complicated encryption strategy.

[7] The Ponemon Institute, “Lost Customer Information: What Does a Data Breach Cost Companies?”, November 2005

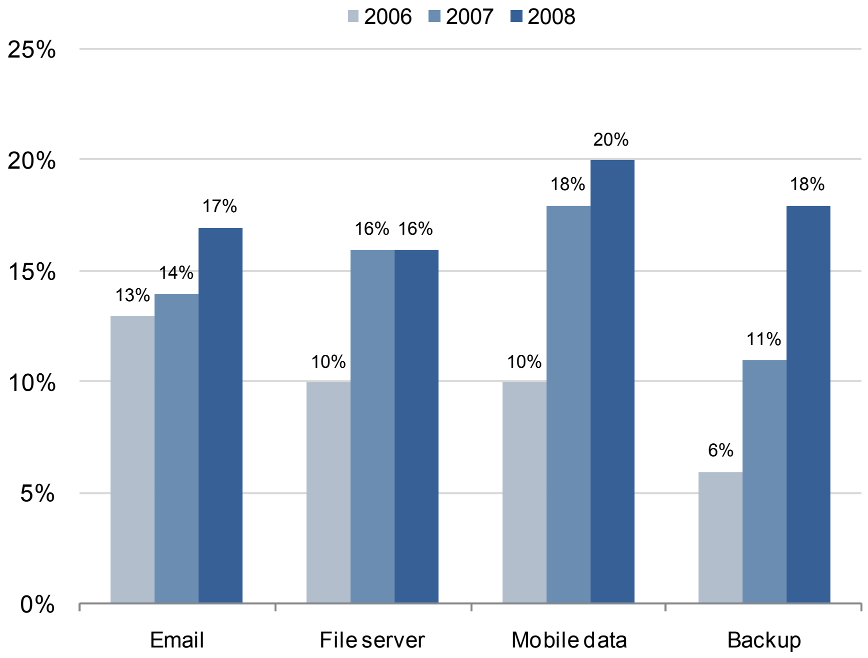

Figure 6: Enterprise encryption use by application type

Respondents reporting encryption application used "most of the time"

Key management budgeted for in 2008, organizations seeking to reduce operational costs. As organizations deploy encryption more broadly across the enterprise, the importance of managing deployments grows. Key management, including the active management of encryption key lifecycle, policy, and reporting, enables user account provisioning, encryption application operation, corporate access to encrypted data, and ongoing reporting for compliance. Without effective key management, the costs of deploying and maintaining encryption could outweigh the benefits of enterprise data protection and risk mitigation.

Organizations surveyed on average plan to spend 34 percent of their total encryption budget on key management solutions. Figure 7 on page 14 shows that the largest segment plans to spend between 21 to 40 percent of their encryption budgets on key management.

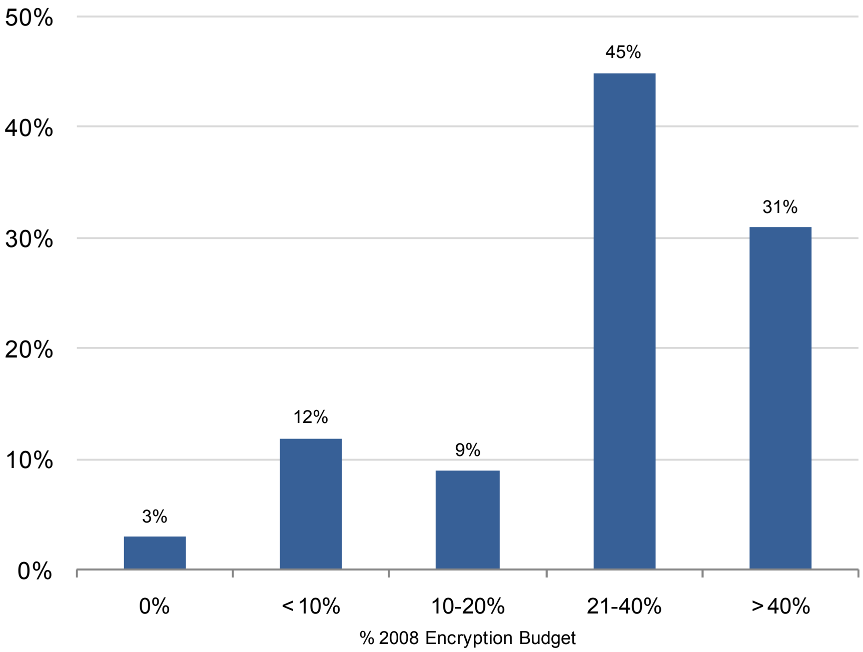

Figure 7: Percentage of 2008 encryption budget earmarked for key management

While key management solutions are an expense, 45 percent of organizations expect their key management investments to reduce the overall operational costs of enterprise data protection. Figure 8 shows that only 6 percent of organizations expect key management to increase the operational costs of enterprise data protection.

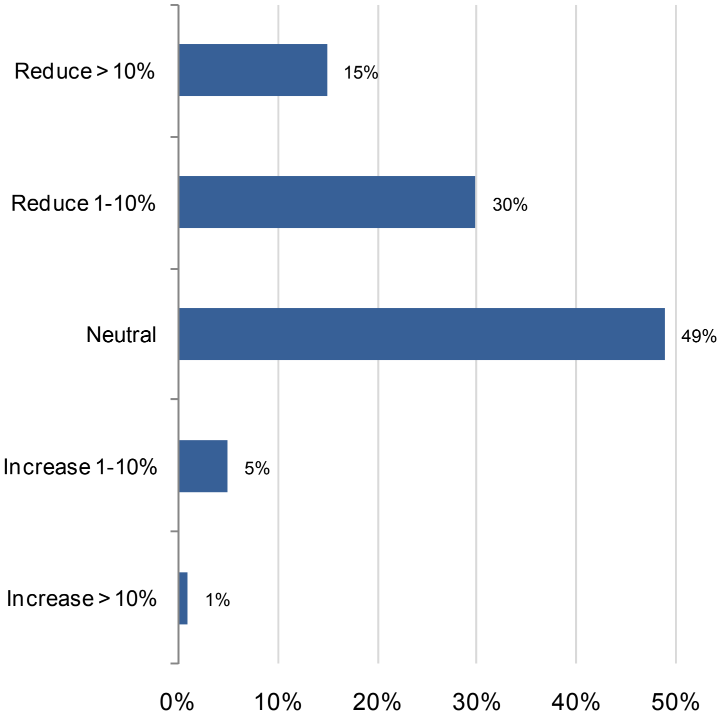

Figure 8: Impact of key management on overall costs of enterprise data protection

Single enterprise vendor for key management preferred. Products for key management are available that manage only a single encryption key type (e.g. disk encryption or tape backup) or manage different type of encryption keys for different applications (this approach is commonly referred to as an encryption platform approach). In this survey, 58 percent of organizations expect to deploy a single enterprise-wide key management solution or deploy a single vendor's key management solution for different purposes in 2008 (see Table 3). Only 13 percent of organizations are seeking a tactical key management product for just one encryption application.

Benefit	Total %
Single enterprise-wide solution	11%
Single vendor solution for different purposes	47%
More than one product from different vendors	30%
One point key management application	13%

Table 3: Enterprise preference for key management purchases in 2008

Overwhelming interest in a platform approach. Survey respondents had a very positive view of the encryption platform approach for enterprise deployment. To ensure all respondents had a similar understanding of this approach, the Institute provided them with a definition of an encryption platform. The full definition can be found in the Appendix, beginning on page 20, which speaks to the ability to centrally manage and deploy multiple encryption applications with consistent policy enforcement instead of making inconsistent usage and policy decisions for separate encryption applications.

After reading this definition, respondents rated the importance of the following five significant features of the encryption platform approach:

1. Encryption policy enforcement is automated across all applications
2. Key encryption management activities are automated
3. Encryption tools integrate with third-party applications
4. Encryption program is administered through one interface for all applications
5. Administrators install management interface only once, adding other encryption applications, as needed

Figure 9 on page 16 shows respondents' feedback for 2008 compared to 2007. The bars represent the percentage of respondents that found the features "important" or "very important". For example, 75 percent of respondents felt that having encryption policy enforcement automated across all applications was either important or very important. This feature increased in importance 7 percent for 2008. The high percentages attributed to all five features are compelling evidence that a platform approach meets the key needs of an enterprise IT organization.

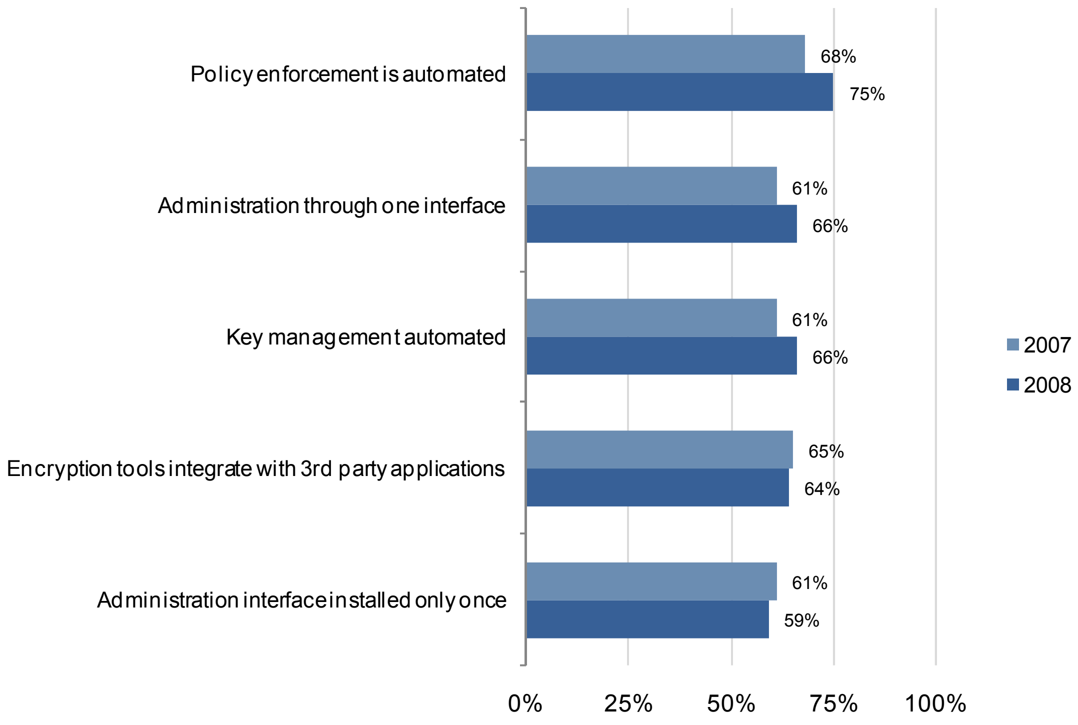

Figure 9: Respondents rate interest in encryption platform attributes

Respondents reporting encryption platform features as "important" or "very important"

Effective IT leaders seek a platform approach. The respondents who rated all five features in Figure 10 as very important are a group with a very high average SES, especially when compared to the average SES of the respondents who rated all features as irrelevant. This group—organizations that made sound IT security decisions in the past—see the most value in an encryption platform solution.

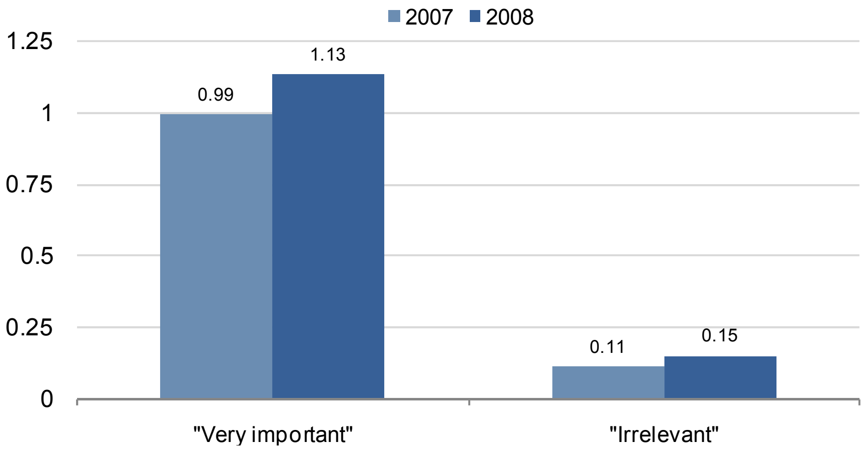

Figure 10: Effective IT leaders (high SESs) see value in encryption platform approach compared to less-effective IT organizations

Respondents see efficiency and cost savings in platform approach. Figure 11shows what respondents perceive to be the key benefits of an encryption platform solution for 2008 compared to 2007. In 2008, the top benefit shifted to the reduction of operational costs, followed closely by the flexibility to add other encryption applications as needed and elimination of redundant administrative tasks.

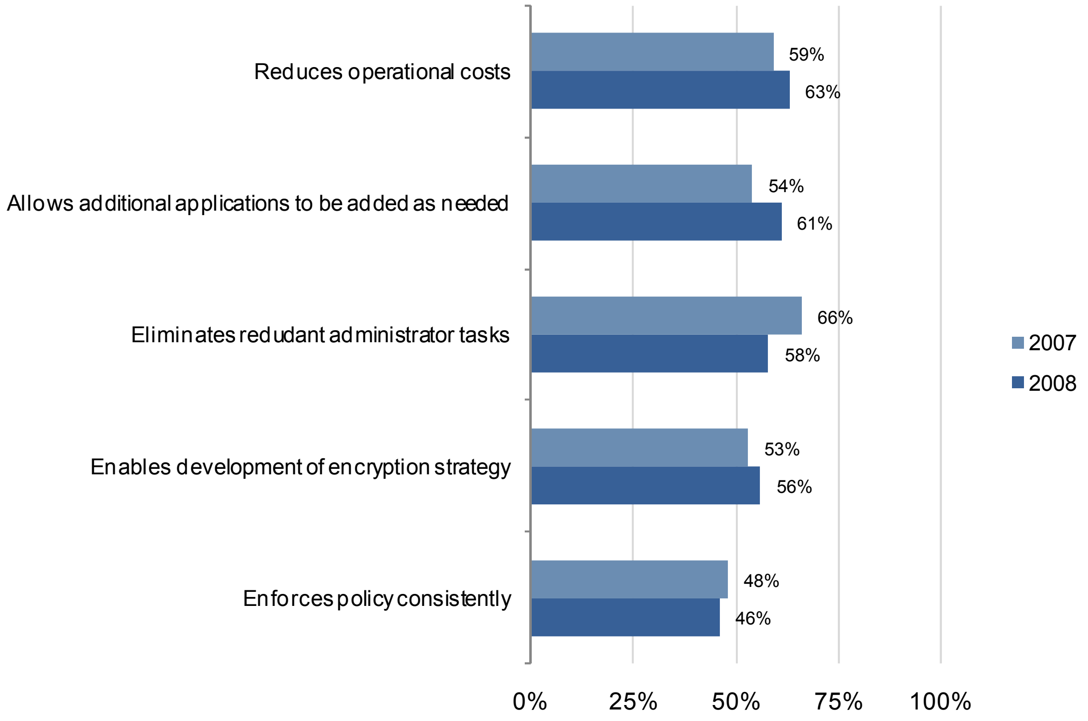

Figure 11: Primary benefits of an encryption platform approach

Report Conclusions

As organizations continue to increase the level of strategic planning for encryption, study results show that effective enterprise data protection programs are making an impact. Not only are organizations defending their data and reducing the risk of data breaches, they are also improving operational cost efficiencies. Key management and the approaches organizations take to managing encryption applications will continue to evolve and given this year’s data it appears will continue to elevate the strategic importance of encryption planning and solutions adoption.

The increased interest in automated policy enforcement, single administration interface, and comprehensive key management continue to favor adoption of an encryption platform solution. While 17 percent of organizations already use an encryption platform approach, another 71 percent of organizations are interested in deploying an encryption platform for their enterprise (total 88 percent either interested or already deployed). The preference for adopting this approach to managing multiple encryption applications from a single console continues to mirror the progression seen with other important enterprise applications such as ERP and CRM, providing further evidence that the encryption platform solution is the next step in the evolution of data security.

About The Ponemon Institute

The Ponemon Institute© is dedicated to advancing ethical information and privacy management practices in business and government. The Institute conducts independent research, educates leaders from the private and public sectors, and verifies the privacy and data protection practices of organizations in a variety of industries.

Dr. Larry Ponemon is the chairman and founder of The Ponemon Institute. He is also a founding member of the Unisys Security Leadership Institute and an Adjunct Professor of Ethics & Privacy at Carnegie Mellon University's CIO Institute. Dr. Ponemon is a critically acclaimed author, lecturer, spokesman, and pioneer in the development of privacy auditing, privacy risk management, and the ethical information management process.

Previously, Dr. Ponemon was the CEO of the Privacy Council and the Global Managing Partner for Compliance Risk Management at PricewaterhouseCoopers (where he founded the privacy practice). Prior to joining PricewaterhouseCoopers, Dr. Ponemon served as the National Director of Business Ethics Services for KPMG and as the Executive Director of the KPMG Business Ethics Institute. Dr. Ponemon holds a Ph.D. from Union College, attended the Doctoral Program in System Sciences at Carnegie-Mellon University, and has a Masters degree from Harvard University as well as a Bachelors degree from the University of Arizona. Contact The Ponemon Institute at www.ponemon.org or +1 800 887 3118.

About PGP Corporation

PGP Corporation is a global leader in email and data encryption software for enterprise data protection. Based on a unified key management and policy infrastructure, the PGP® Encryption Platform offers the broadest set of integrated applications for enterprise data security. PGP® platform-enabled applications allow organizations to meet current needs and expand as security requirements evolve for email, laptops, desktops, instant messaging, smartphones, network storage, file transfers, automated processes, and backups.

PGP® solutions are used by more than 80,000 enterprises, businesses, and governments worldwide, including 95 percent of the Fortune® 100, 75 percent of the Fortune® Global 100, 87 percent of the German DAX index, and 51 percent of the U.K. FTSE 100 Index. As a result, PGP Corporation has earned a global reputation for innovative, standards-based, and trusted solutions. PGP solutions help protect confidential information, secure customer data, achieve regulatory and audit compliance, and safeguard companies' brands and reputations. Contact PGP Corporation at www.pgp.com.

Appendix

Definition of an Encryption Platform Approach

An encryption platform reduces the complexity of protecting business data by enabling organizations to deploy and manage multiple encryption applications from a single console. A platform-based solution allows organizations to quickly deploy encryption for new applications, as needed. For example, a company can deploy email encryption. Then, it might choose to deploy whole disk encryption clients to all laptop users. Subsequently, the platform provides solutions for deploying end-to-end storage encryption for engineering, human resources, finance, legal, and other core functions that use sensitive or confidential information. The entire deployment is managed from a single administration interface using centrally defined encryption policies to automate encryption and add new users and applications, as needed.

Security Effectiveness Score

The following 24 attributes are used to describe an effective IT security based on responses from survey participants. These attributes comprise an organization's Security Effectiveness Score (SES).

1. Identify major data breaches involving sensitive or confidential information
2. Determine the root causes of major data breaches involving sensitive or confidential information
3. Know where sensitive or confidential information is physically located
4. Secure sensitive or confidential data at rest
5. Secure sensitive or confidential data in motion
6. Secure endpoints to the network
7. Identify system end users before granting access rights to sensitive or confidential information
8. Protect sensitive or confidential information used by outsourcers (including third parties, affiliates, and business partners)
9. Prevent or curtail major data breaches involving sensitive or confidential information
10. Prevent or curtail hacking attempts to acquire sensitive or confidential information
11. Prevent or curtail denial-of-service attacks
12. Limit physical access to data storage devices containing sensitive or confidential information
13. Demonstrate the economic value or other tangible benefits of the company's IT security program
14. Ensure minimal downtime or disruptions to systems resulting from security problems
15. Comply with legal requirements and policies (including privacy laws and statutes)
16. Conform with leading self-regulatory requirements such as ISO 17799, PCI, and others
17. Prevent or curtail viruses, worms, Trojans, and spyware infections
18. Perform timely updates for all major security patches
19. Control all live data used in systems development activities
20. Enforce corporate policies, including the termination of employees or contractors who pose a serious insider threat
21. Attract and retain high-quality IT security personnel
22. Training and awareness program for all system users
23. Conduct independent audits of the system
24. Consistently manage security program administration