

---

# Enterprise Encryption in the Financial Services Sector

*Why Organizations Struggle to Bridge the Gap  
Between Compliance Requirements and Capabilities*

Lane F. Cooper  
Director  
InfoTech: The Telecom Intelligence Group  
lcooper@accessintel.com  
Tel: 415 699 9334

## Enterprise Encryption in the Financial Services Sector

Why Organizations Struggle to Bridge the Gap  
Between Compliance Requirements and Capabilities

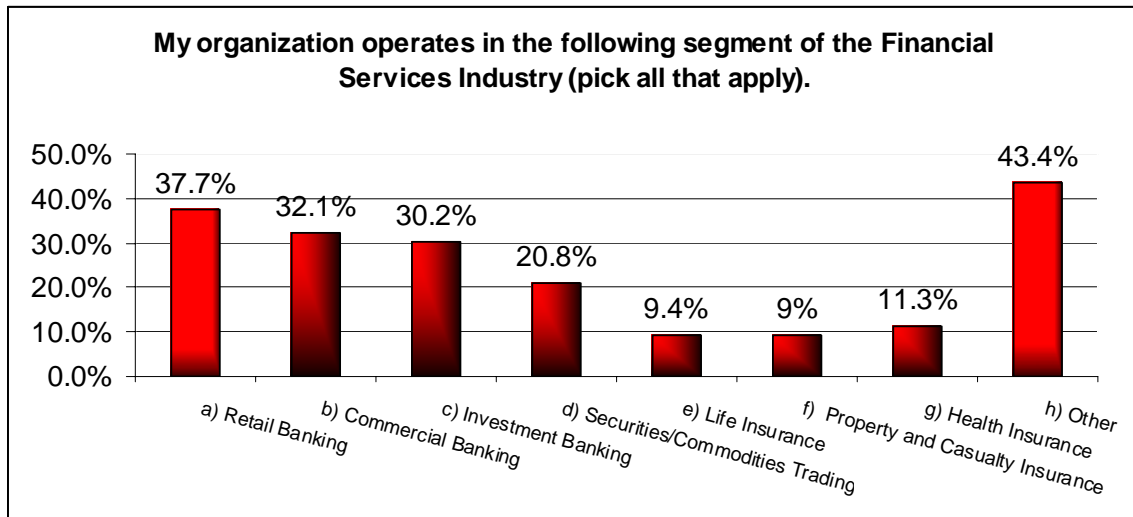
By  
Lane F. Cooper  
Director

*InfoTech: The Telecom Intelligence Group*

### Introduction and Summary of Findings

While there is a growing appreciation for the role that enterprise-wide encryption strategies ought to play in financial-services institutions, a survey of IT and security professionals at 112 financial services companies in the United States conducted by **InfoTech: The Telecom Intelligence Group** reveals that the industry lacks confidence in its current ability to implement and maintain such strategies.

Conducted during two weeks in January 2006, the survey of senior IT managers and executives who have responsibility for enterprise systems and security shows there are growing competitive and regulatory pressures to encrypt and then to develop an enterprise-wide approach to encryption. (NOTE: The survey included senior technical managers at consulting and systems-integration organizations tasked with maintaining enterprise systems and security for financial-services organizations.)



**Source:** *InfoTech: The Telecom Intelligence Group*

However, there is a “disconnect” between these pressures and current levels of encryption activity in the industry. The survey reveals significant barriers that must be overcome to accelerate the adoption of enterprise-wide encryption strategies. Chief among them is the need to automate the process of encrypting and decrypting “data at rest” throughout the stages of the information life cycle.

This gap represents both a challenge and an opportunity for players in the financial services industry.

- The challenge revolves around the need to address the significant vulnerabilities to which many players in the sector admit they are exposed.
- On the other hand, low levels of encryption adoption in the industry offer an opportunity for financial institutions to establish competitive differentiation on an issue that matters very much to both corporate customers and consumers.

While the industry currently is in the early adopter stage of enterprise-wide encryption deployment, the survey shows that the compelling drivers – combined with the availability of technology solutions that manage the complexity of deployment – will accelerate during the next two or three years. It will be a short-lived point of differentiation, however.

It is the conclusion of this report that, by the end of the decade, enterprise-wide encryption practices will be a competitive requirement for organizations throughout financial-services industry.

### **Survey Report Objectives**

As we set out to develop this survey report, our objective was three-fold:

- To identify key drivers and barriers for enterprise-wide encryption strategies in the financial-services industry;
- To assess where encryption currently is being used by the sector; and
- To understand the future plans that the industry has for encryption as an element in security initiatives to protect enterprise systems in general...and data at rest in particular.

(NOTE: An appendix with the full survey results is available at the end of this report.)

### **Key Findings**

- **Compliance pressure is the key driver of enterprise-wide encryption strategies throughout the financial sector.** A full 87 percent of respondents reported that regulatory and legislative compliance is elevating the requirement to encrypt sensitive information in their organizations' enterprise systems. Of the regulations that loomed largest from a compliance standpoint:
  - 70 percent cited Sarbanes Oxley.
  - Approximately 67 percent were governed by Gramm Leach Bliley.
  - The Patriot Act affected more than 60 percent of respondents.
  - Half of the respondents (49 percent) were affected by California's SB1386 legislation or other state privacy laws.

We were struck by this last finding regarding the California regulation. It was cited nearly as much by institutions that were not operating in that state as those that were. The consensus is that the requirement to publicly disclose and notify those affected by a security breach that compromises personal and financial data will be adopted by other states and/or will become a federal requirement in the coming months and years.

Regulatory compliance trumped “executive mandates” and “recent security breaches” as drivers for more extensive use of encryption in their organizations in 2006.

- 67 percent indicated that compliance requirements were putting their organizations under more pressure to encrypt data at rest.
- 31 percent – less than one-third – cited “executive mandates” as an encryption driver.
- Only 18 percent of respondents said recent breaches in security were a factor in using encryption to protect data at rest.
- **In terms of barriers, there are serious questions about the impact encryption technology will have on enterprise systems and day-to-day business operations.** The industry appears to have major questions about the practicality of enterprise-wide encryption.
  - 59 percent of the respondents reported the technical impact of encryption on existing applications was a serious concern.
  - 55 percent worry about the impact encryption strategies may have on overall enterprise-system performance.
  - 51 percent believe the cost of implementing an encryption strategy across the enterprise may be prohibitive.
- **Current encryption practices in the financial-services industry are spotty at best.** Encryption as a distinct discipline is only just now beginning to resonate as a potential strategic area of focus in an overall information-assurance strategy. But in the meantime, feelings about encryption in this industry are ambivalent.
  - 54 percent of respondents reported encrypting data at rest is a high priority for their organizations. However, digging a bit deeper into the data, only 17 percent of participants “strongly agreed” with the statement. So, in terms of mood, it was not the most confident statement of support for this proposition.
  - Less than a third, only 31 percent, believe their organizations are doing an adequate job of encrypting data at rest.

- In fact, more than a third (38 percent) effectively believe their organizations are doing an **inadequate** job of protecting data at rest with encryption.
- This left the remaining third to admit they simply do not know how to judge their organizations' performance.

In the meantime, the main focus of encryption activity is on data at the application level.

- 62 percent of respondents say they currently are using encryption to protect sensitive customer data at the "application" level.
  - 54 percent are encrypting customer data stored on disks.
  - 52 percent report that efforts currently are in place to harness encryption to protect customer data at the "database" level.
  - 50 percent are encrypting customer data at the "file" level.
  - Only 35 percent, however, are encrypting information stored on tape.
- **Encryption clearly ranks way behind other security initiatives as a "strategic" element in the overall security mix of the financial-services industry.** Encryption must be elevated to the same level of importance as authentication and authorization practices if it is to be integrated effectively into the security fabric of the industry. Compare the ambivalent feelings about encryption with the following:
    - 87 percent of respondents say their organizations have rigorous programs in place to enforce authentication verification.
    - 86 percent indicate they routinely and carefully manage authorization protocols to help ensure role-based access to information.
  - **The financial-services sector is moving forward with more stringent plans for encryption.** It seems the industry is approaching a tipping point when it comes to encryption.
    - 57 percent of respondents say they plan to bring more resources to bear on efforts to encrypt data at rest in 2006 (compared with 2005).
    - 30 percent report there are no current plans in place to buttress encryption initiatives.

With more than half of the respondents actively exploring a more robust role for encryption in the enterprise, it is reasonable to expect it will shortly (within 18 to 24 months) become a higher-profile and more standard element of the security mix in this industry.

## **Conclusion**

The financial-services industry continues to labor under a “perimeter protection and prevention” mentality when it comes to data security. It is confident in the security initiatives it has in place to keep hackers and other threats to data from penetrating defense measures.

But given the fact that most organizations are destined to suffer some sort of major breach in security (from either internal or external sources), the lack of encryption represents a misunderstood area of vulnerability.

A clear case must be made for a more strenuous approach to encryption as the last line of defense in the event that other prevention initiatives are breached.

It will also be important for encryption to demonstrate it can deliver measurable improvements in the industry’s security posture and that it can be harnessed to cost-effectively comply with the broad array of privacy regulations the financial industry must address.

### **About InfoTech: The Telecom Intelligence Group**

**InfoTech: The Telecom Intelligence Group** is a global business-intelligence resource for decision makers among technology developers, service providers, manufacturers, resellers/systems integrators and enterprises of all sizes. InfoTech publishes quarterly tracking and analysis reports on business communications systems and applications as part of its “InfoTrack for Enterprise Communications” (IEC) program. For more information, visit: [www.telecomweb.com](http://www.telecomweb.com).

### **About the Sponsor: Ingrian Networks**

This survey report was sponsored by Ingrian Networks, which brings complete data privacy to the enterprise. With Ingrian DataSecure Platforms, organizations can protect critical data from both internal and external threats, thus ensuring compliance with legislative and policy mandates for security. DataSecure features a dedicated security appliance and specialized software that enables organizations to encrypt critical data in applications and databases. With its capabilities for granular encryption, seamless integration and centralized security management, DataSecure enables organizations to guard against a range of security threats with unparalleled ease and cost-effectiveness.

Ingrian is a privately held company backed by such investors as Globespan Capital Partners, HighBAR Ventures, Menlo Ventures, Partech International and Prism Venture Partners. For more information, visit: [www.ingrian.com](http://www.ingrian.com).

APPENDIX: Encryption in the Financial Services Industry Survey Results

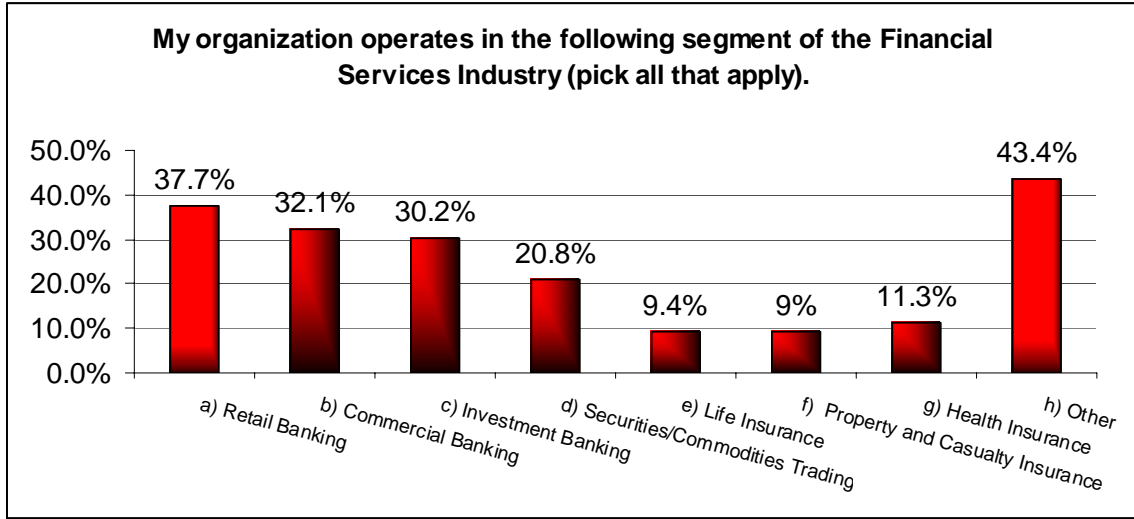


Diagram 1

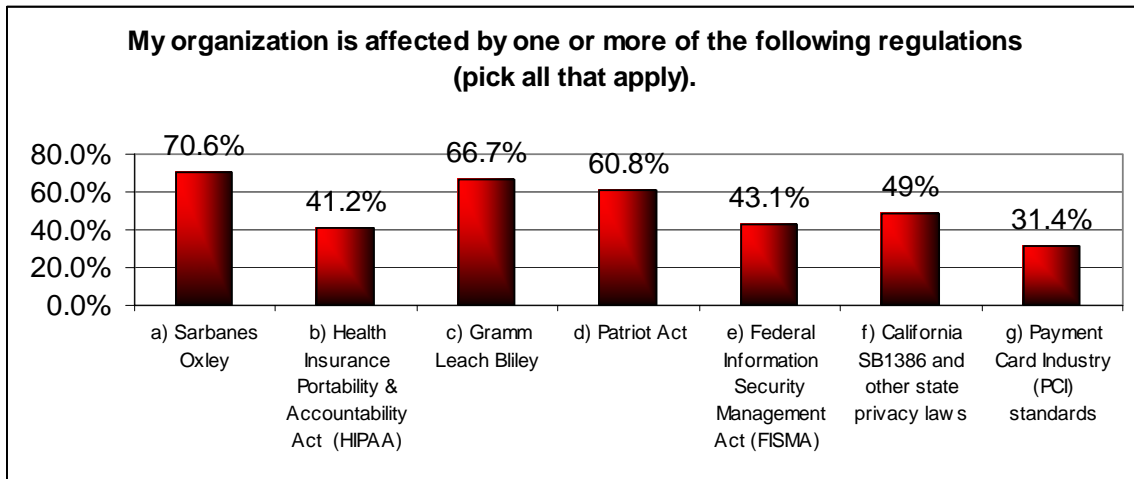


Diagram 2

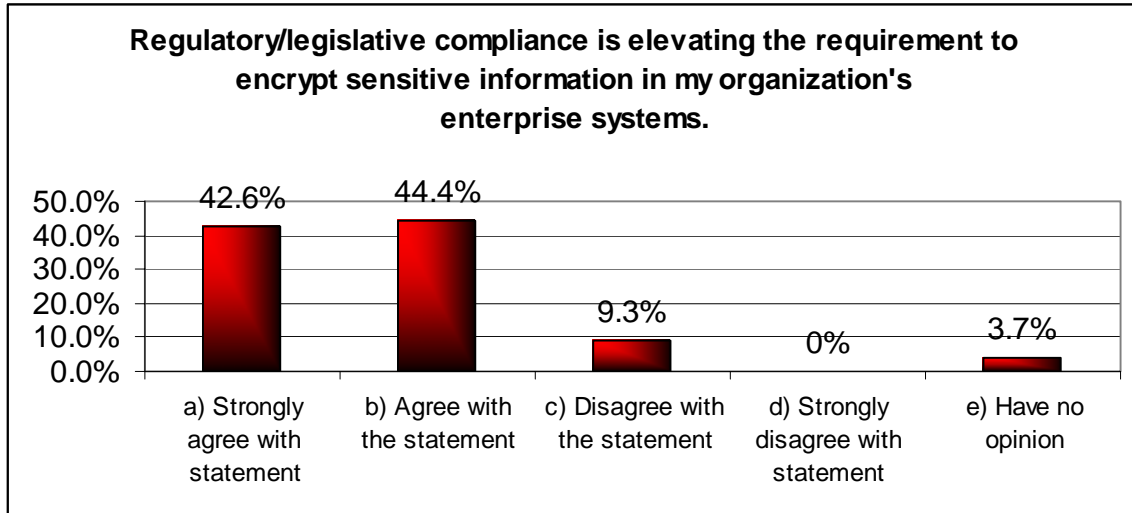


Diagram 3

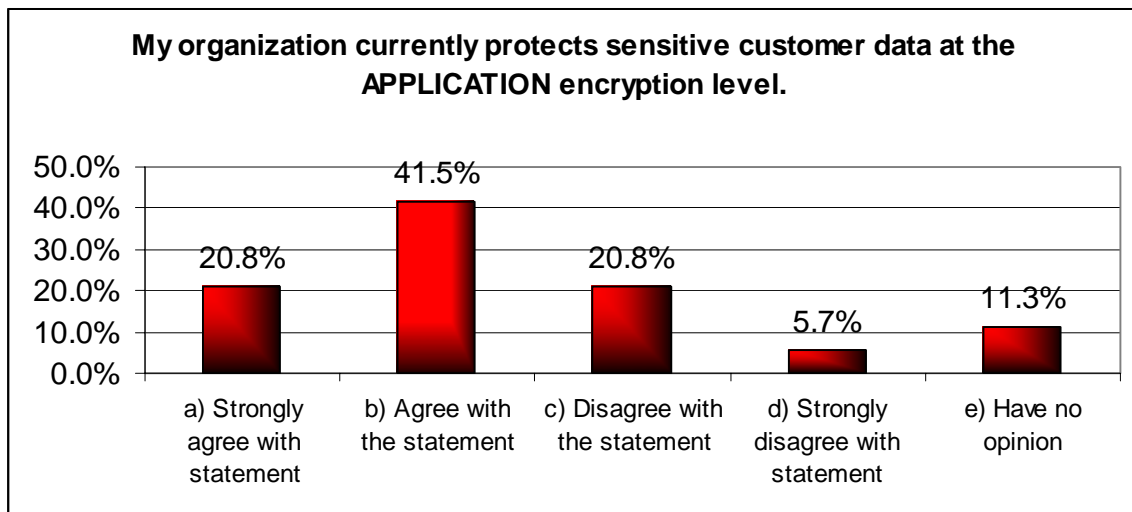


Diagram 4

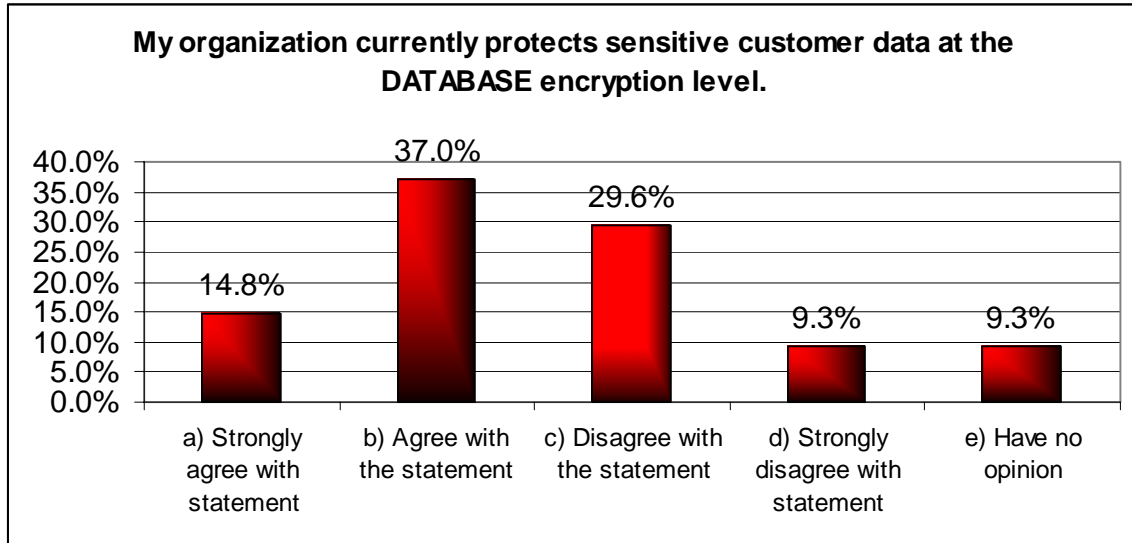


Diagram 5

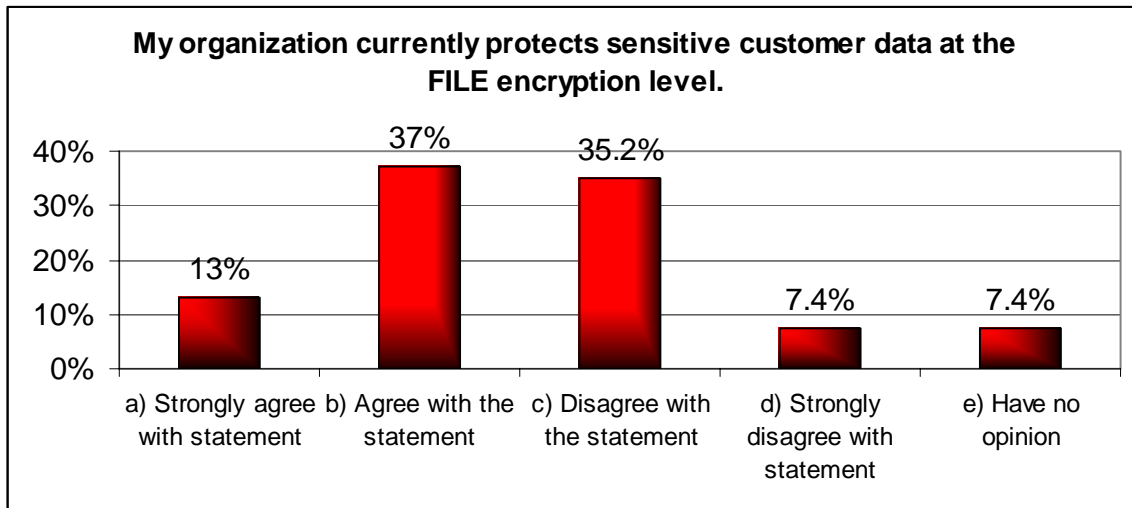


Diagram 6

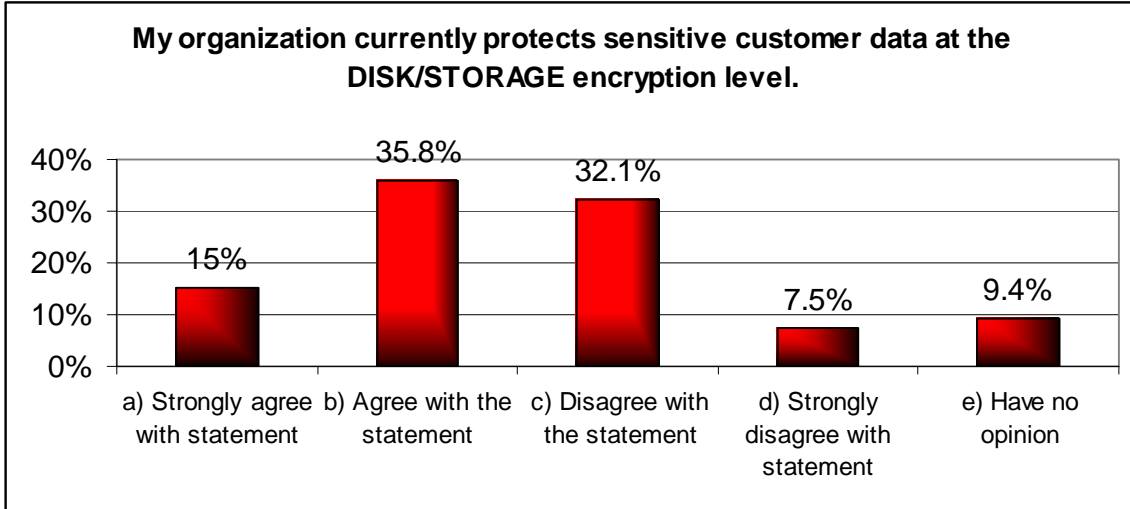


Diagram 7

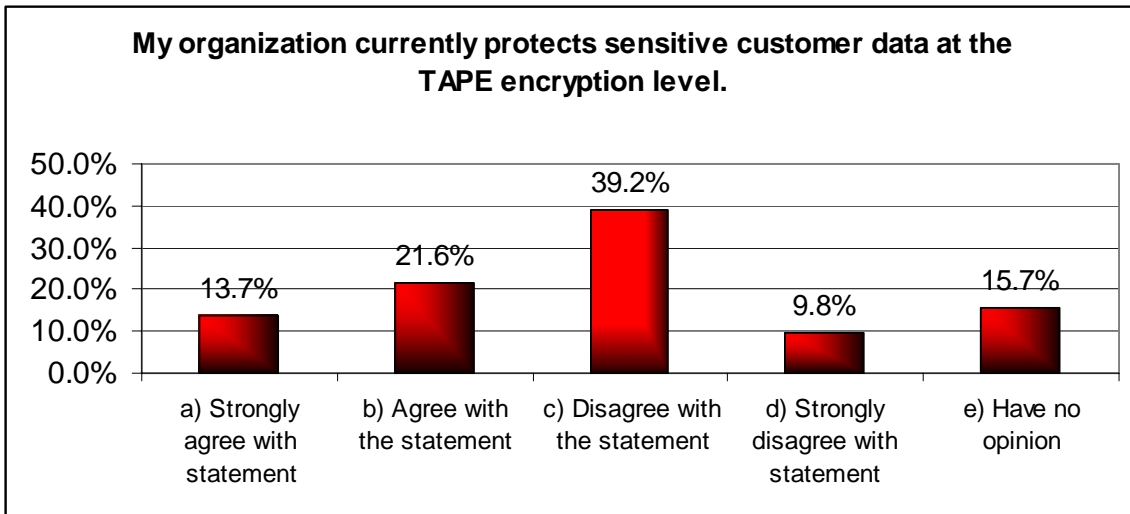


Diagram 8

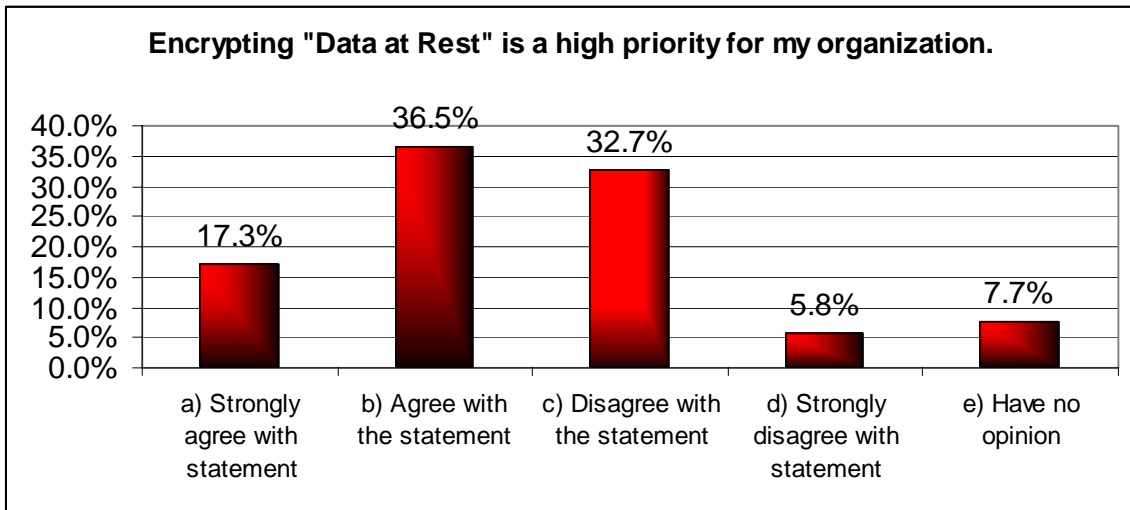


Diagram 9

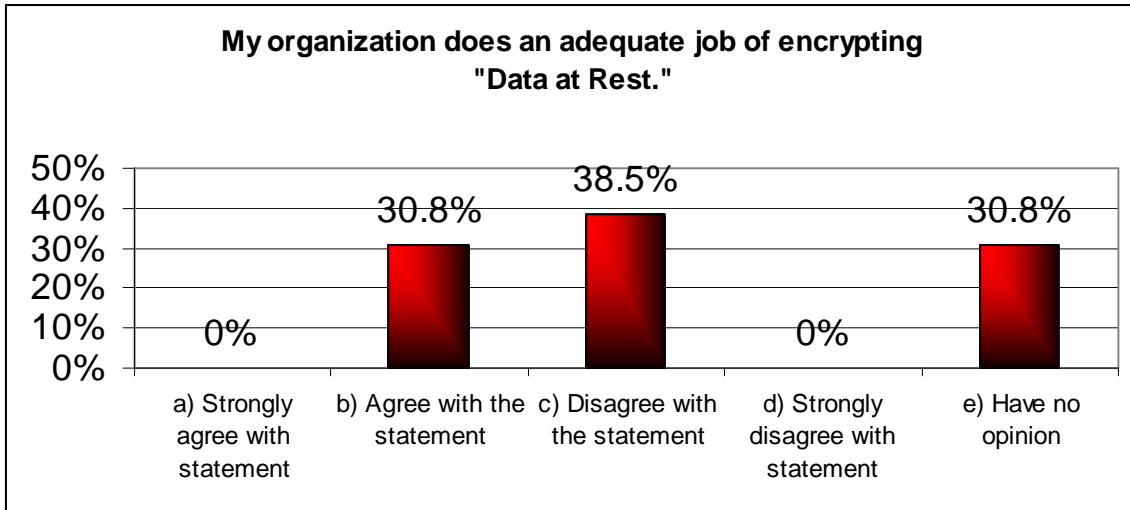


Diagram 10

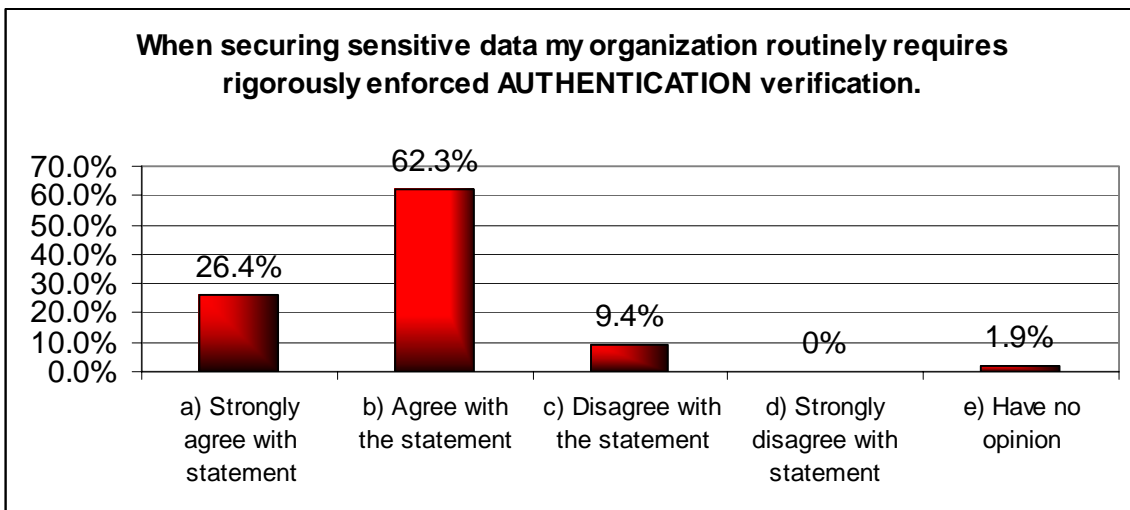


Diagram 11

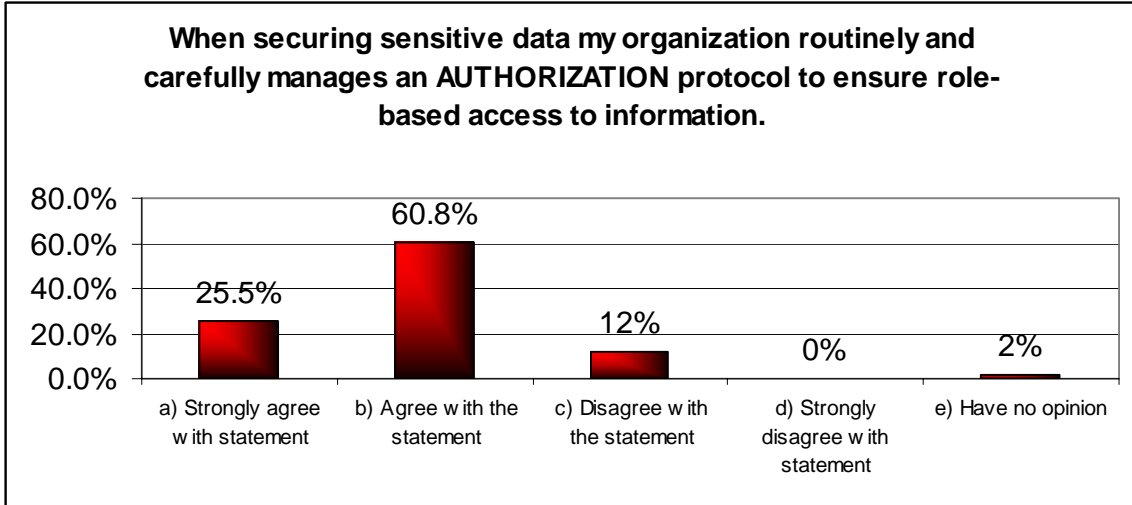


Diagram 12

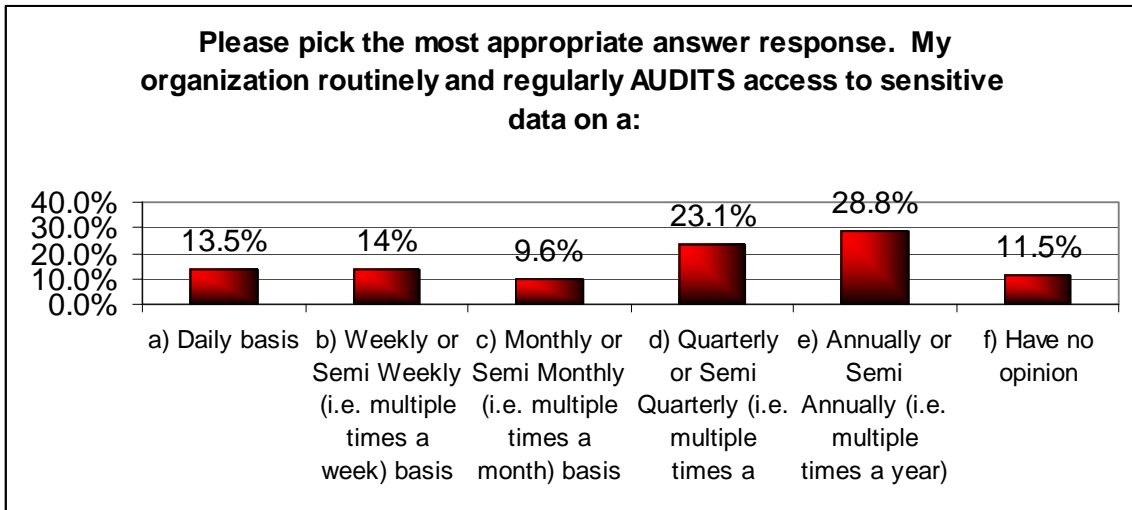


Diagram 13

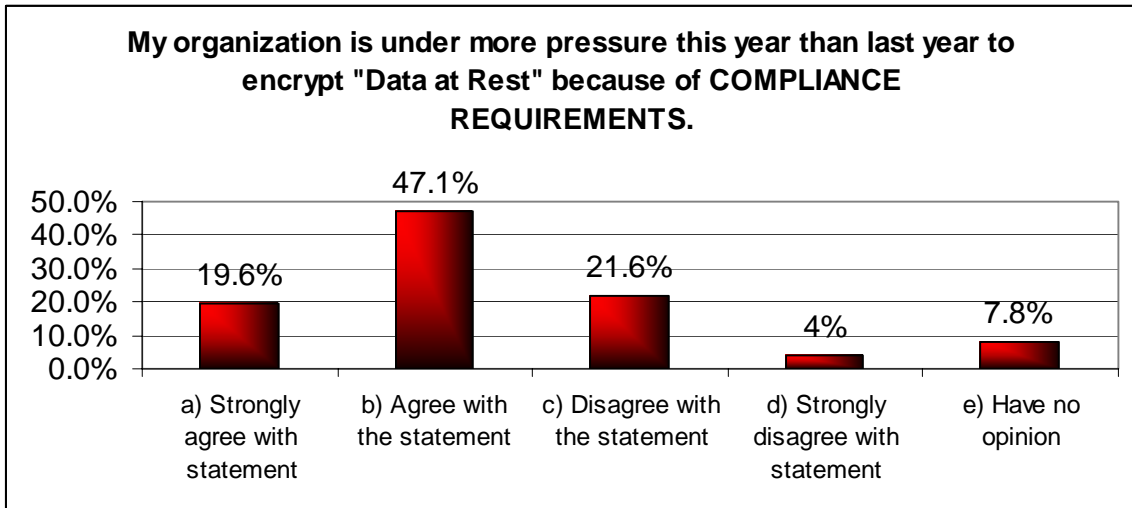


Diagram 14

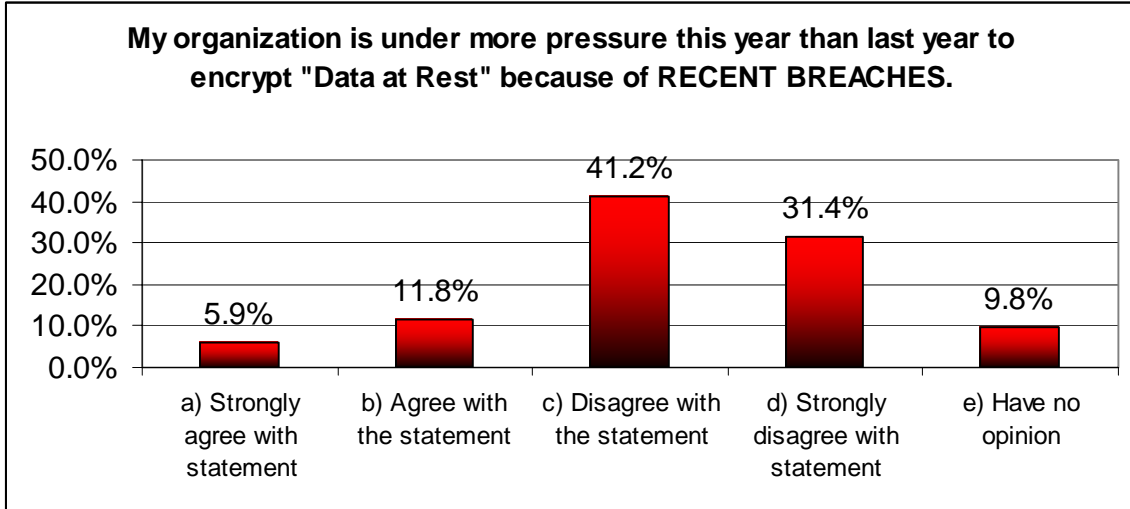


Diagram 15

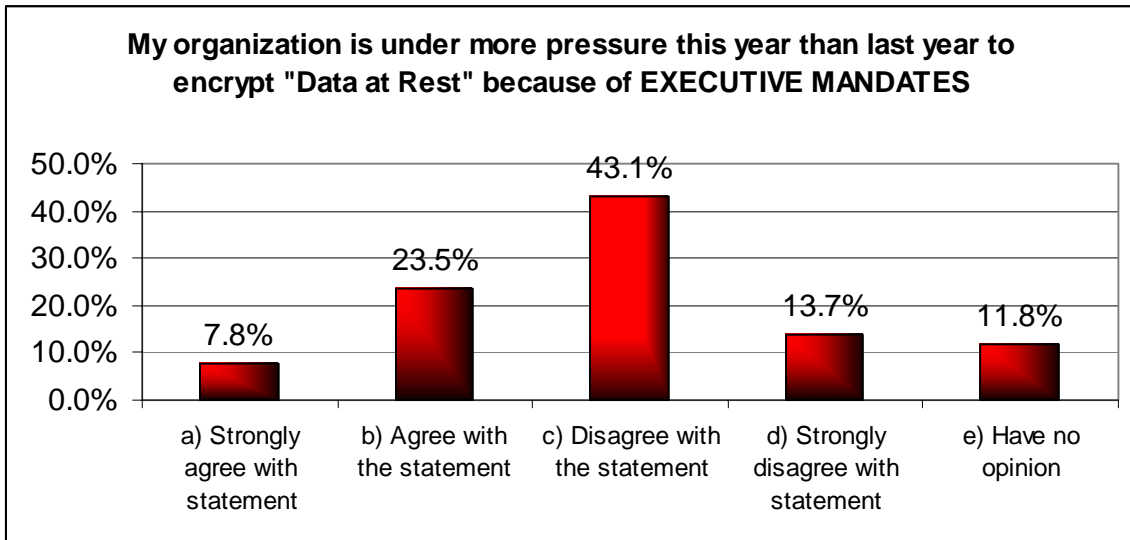


Diagram 16

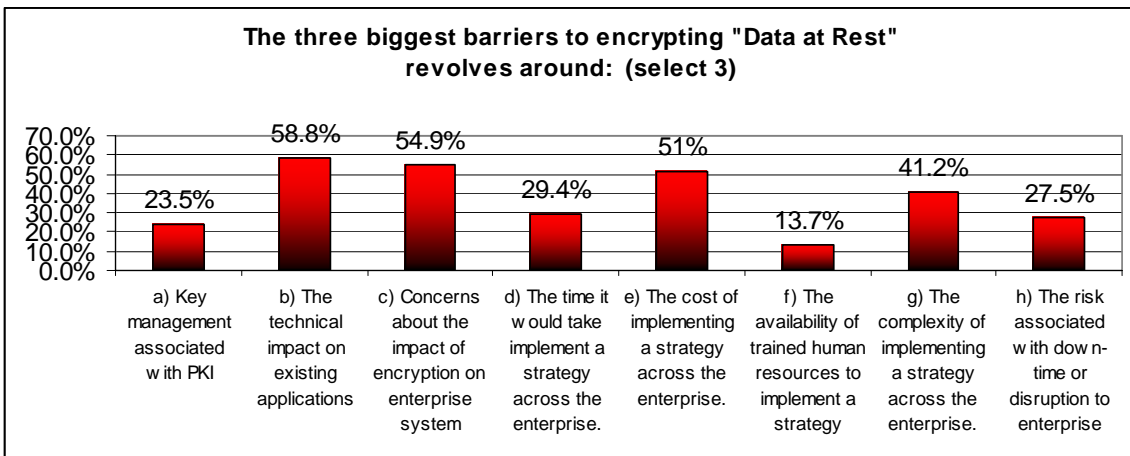


Diagram 17

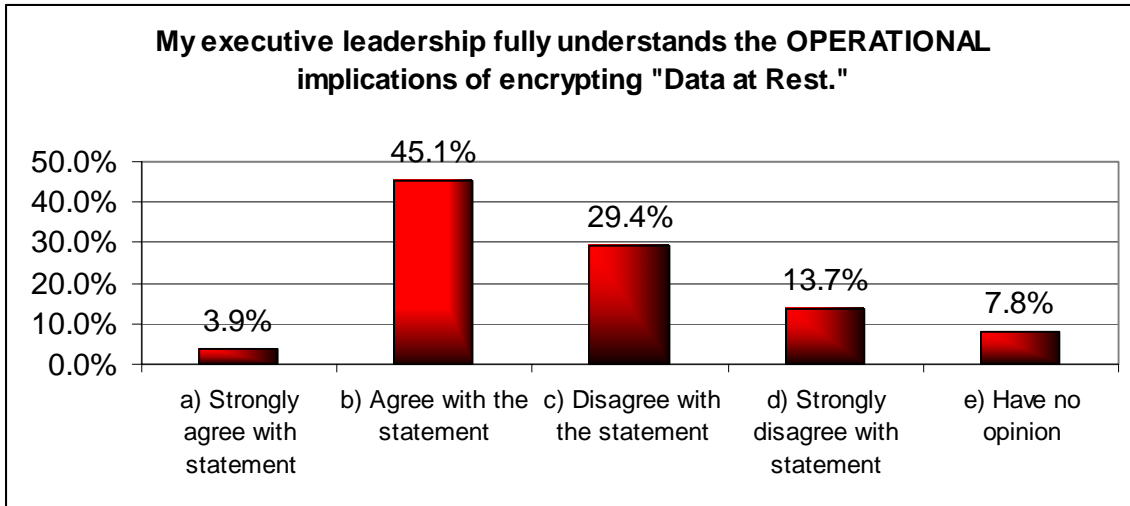


Diagram 18

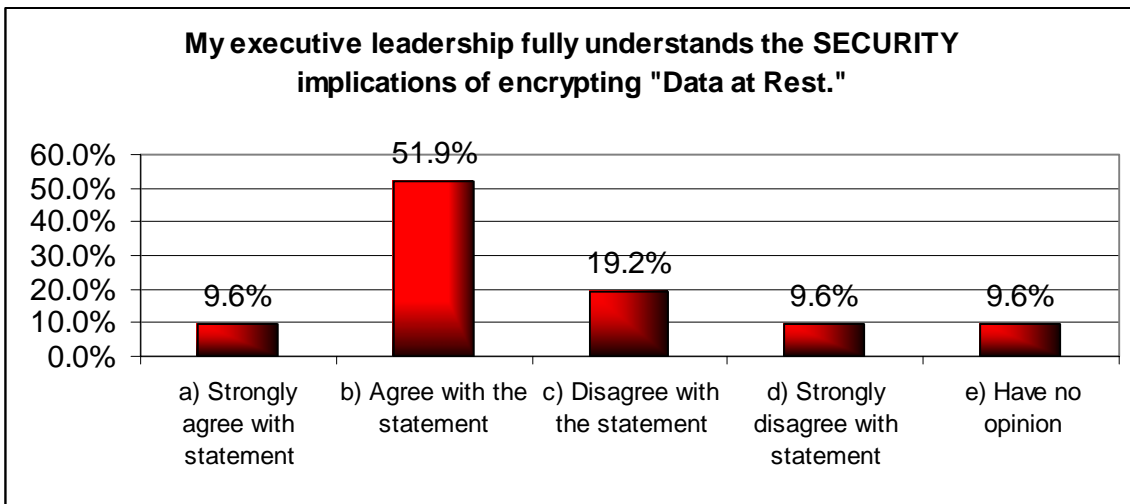


Diagram 19

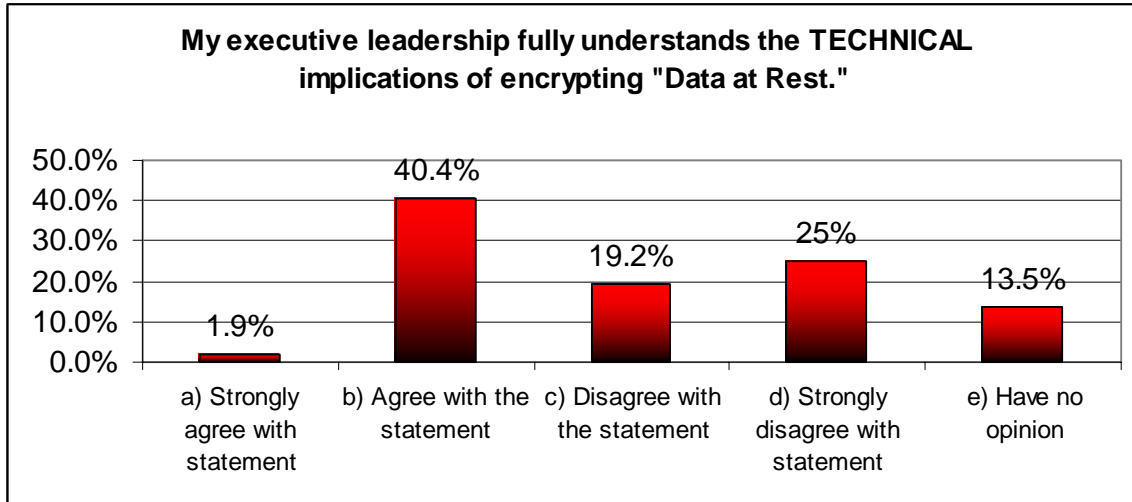


Diagram 20

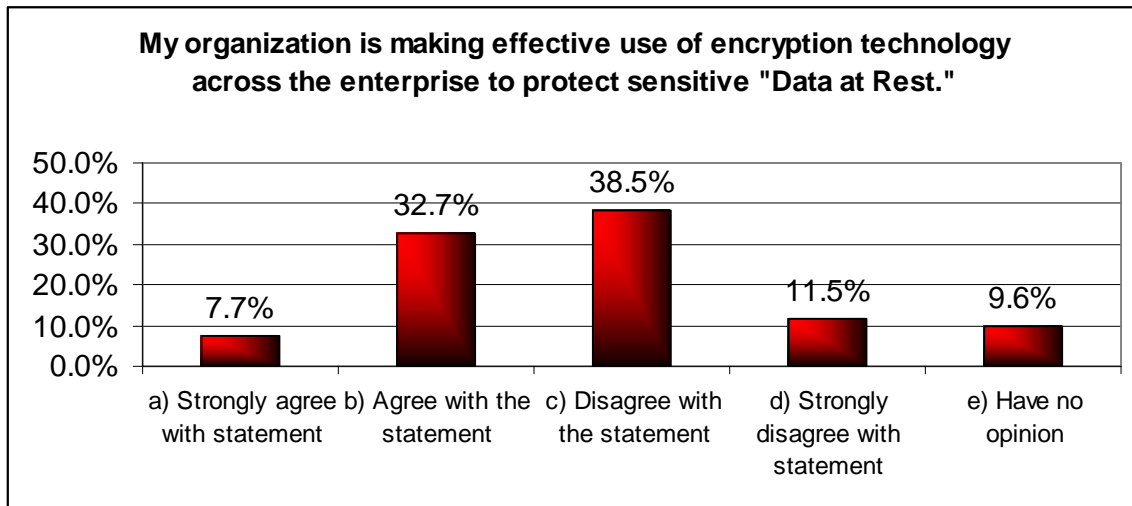


Diagram 21

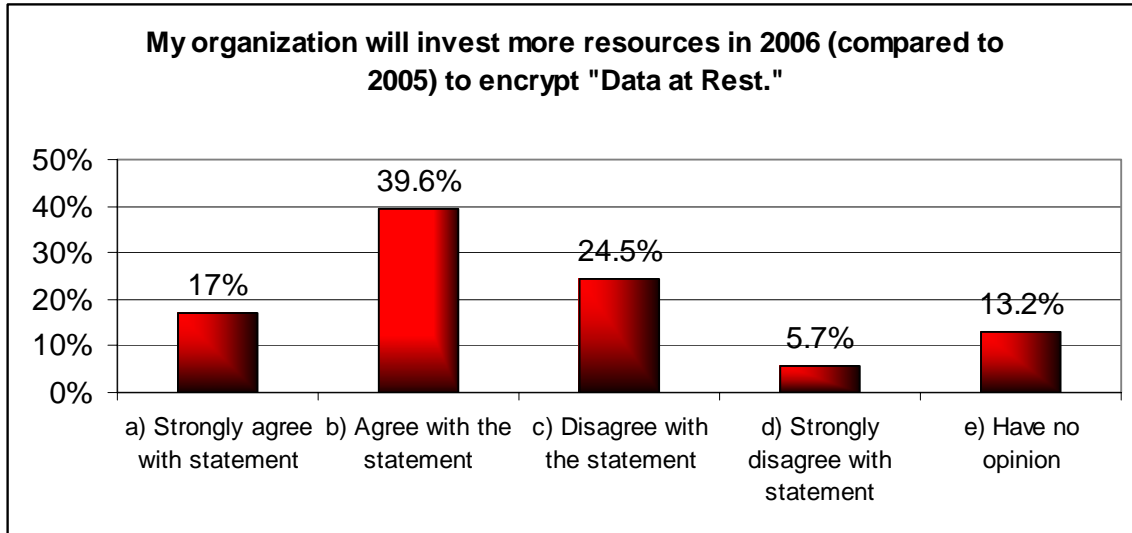


Diagram 22