2009 Encryption and Key Management Industry Benchmark Report

A risk management benchmark for data protection

Author: Kimberly Getgen, Principal, Trust Catalyst

October 20, 2009

trust catalyst

Foreword: Risk Management for Data Protection

Dear data security professional,

Where does your organization's risk management strategy stand when it comes to data protection? Despite a growing emphasis on encryption and related issues, few organizations have had the hard data needed to benchmark their risk management efforts against industry standards. Until now.

As a leader in encryption and key management, Thales wanted to provide the industry with a much-needed benchmark. We engaged Trust Catalyst, a research firm, to conduct a survey of industry professionals and report the findings. I found the resulting *2009 Encryption and Key Management Industry Benchmark Report* fascinating. I think you will, too. But more importantly, it's a tool your organization can use to learn where it stands in relation to industry standards and emerging trends.

After reading the report, I was struck by two things in particular: Organizations have made great strides in protecting sensitive data *and* there is more to do, especially with regard to managing encryption keys and protecting backup tapes.

The next great hurdle in encryption is protecting all sensitive data—not just some of it. Many of the respondents to the survey are progressing in that direction, while others are advancing more slowly. Either way, we all have the opportunity to learn from their collective experiences.

I want to thank all of you who participated in the survey for sharing your time and insights. I also want to thank the Thales customers and partners who have helped to make us an industry leader. At Thales, we are pleased to be able to sponsor this report, and we hope that all of you will find it to be a valuable benchmarking tool.

Best regards,

Bryta Schulz

Vice President, Product Marketing
Thales Information Systems Security

trust catalyst

Table of Contents

www.trustcatalyst.com
Telephone: +1. 415. 867.8842
Contact: info@trustcatalyst.com

Executive Summary

Data protection is an exercise in risk management. Adequately protecting data and managing compliance must be balanced with operating efficiency and profitable growth. Getting this combination right is more important than ever. The second annual *Encryption and Key Management Industry Benchmark Report* investigates how IT security managers are addressing these challenges and provides recommendations to help you reassess your strategy in light of the new data protection imperative.

Since publication of the *2008 Encryption and Key Management Industry Benchmark Report*, demands to protect data have only grown. New data breach notification laws and the codification of industry-specific standards have made the protection of data an even higher priority.

In the US, HITECH (Health Information Technology for Economic and Clinical Health Act) rules introduce data breach notification requirements nationally for healthcare data. US state rules in Massachusetts (MA 201 CMR 17) and California (CA SB 1386) are mandating the use of encryption to protect data. Nevada's NV SB 227 went even further by mandating compliance for the industry-developed Payment Card Industry Data Security Standard (PCI DSS) for those accepting credit cards. In Germany, the Federal Data Privacy Act mandates data breach notification for the first time. And in the UK, aggressive action by the Information Commissioner Office (ICO) and Financial Services Authority (FSA) has made data breach notification de facto law.

Over the next 12 months, regulation requiring the protection of data and mandatory breach notification will only continue to grow. At the same, many organizations will continue to experience damaging, costly, and very public data breaches. As this survey shows, encryption is one of the most effective means to protect data. Using encryption with automated key management goes a long way toward helping organizations achieve their compliance and IT operations objectives.

Key Findings

Trust Catalyst conducted the second annual data protection survey to evaluate evolving trends in encryption and key management. This report, sponsored by Thales, provides new analysis and unique data to help organizations learn from the data protection and risk management decisions of their peers.

The report identifies these key findings:

- **Unnecessary risk.** The Achilles' heel of many organizations remains the same as last year: unencrypted databases and backup tapes. Less than 50 percent of organizations are encrypting backup tapes and databases, creating a critical vulnerability in data protection programs. Nearly 20 percent of participants who are not encrypting backup tapes said their organization would wait until a breach occurred before beginning to encrypt tapes.

- **Cost of encryption remains a top concern.** Participants said cost remains the single most important factor preventing the encryption of data that should be encrypted. Over half cited either the cost of

the encryption solution (26 percent) or the cost of managing the encryption solution (25 percent) as the primary obstacles to adopting encryption where it is needed most.

- **Operational concerns delay encryption projects.** Cost isn't the only barrier to encryption adoption. The decision to encrypt requires organizations to weigh other operational efficiencies against the need for data protection. When asked what was preventing them from encrypting databases, 25 percent of participants cited performance as the key inhibitor. For backup tapes, the complexity of managing keys was the primary obstacle, cited by 24 percent of respondents. Here, many participants told us "availability is more important than confidentiality."

- **Lost keys disrupt business.** 8 percent of organizations have experienced problems with lost encryption keys, creating security concerns (50 percent), causing data to be permanently destroyed (39 percent), or disrupting the business (39 percent), while 19 percent of respondents said they directly lost business.

- **Key management and compliance.** Planning an organization's key management strategy is no easy feat. A third of survey respondents (34 percent) have been planning their key management strategy for over a year. For the first time, these participants ranked "proving compliance requirements have been met" as the most challenging aspect of key management.

- **New encryption mandates considered helpful to data protection strategies.** Regulations mandating encryption were seen as helpful in moving data protection strategies forward for an overwhelming 71 percent of survey participants, while only 7 percent disagreed, saying these regulations harmed or obstructed their organization's data protection efforts. Encryption mandates appear to be the ammunition many organizations need to help sell their data protection strategies internally. In addition, 66 percent of respondents expect to see more industry regulations outlining data protection guidelines, and 55 percent expect to see more national breach notification laws.

- **Patient and credit card data protection drives encryption spending.** PCI DSS, HIPAA, and the EU Data Privacy Directive are the top three data protection regulations requiring allocation of new encryption budget over the next 24 months. 54 percent of respondents indicated they were allocating budget for PCI DSS, 29 percent for HIPAA and 22 percent for the EU Data Privacy Directive. Data protection rules such as HIPAA and PCI are driving the use of encryption across industries as the need to protect specific types of data grows.

- **Cloud not ready for prime time**. 52 percent of participants cite data security concerns as being the number one barrier preventing their organization from adopting cloud computing. 43 percent of survey participants said they are not currently planning on "moving to the cloud," while another 47 percent said they would wait until data is encrypted before moving. 59 percent said they would want to manage their own encryption keys if encrypted data was moved to the cloud.

About This Paper

This paper is organized into the following four sections:

- Section I: Data Encryption Trends and Obstacles
- Section II: Regulations and Compliance Drivers
- Section III: Cloud Computing
- Section IV: Importance of Key Management in New Data Protection Imperative

Research methodology and information about the survey respondents are outlined in Appendix A.

Section I: Data Encryption Trends and Obstacles

New compliance regulations are pushing the need to encrypt more data than ever before. In this year's survey, we wanted to understand not only what was being encrypted, but also what was preventing organizations from adopting more encryption where it's needed the most. In this section, we summarize these trends by exploring:

- Encryption trends
- Obstacles to encryption
- Key management trends

Encryption Trends

Table 1 compares the 13 applications surveyed in 2008 to show the change in encryption trends from 2008 to 2009. The applications are ranked from most to least widely deployed according to this year's survey results.

Table 1: Applications encrypting data – comparing 2008 and 2009 results

Encryption application	Rank in 2009 survey	Rank in 2008 survey	Change
Web server – SSL	1	1	0
File encryption – server	2	5	+3
File encryption – desktop	3	2	-1
FTP encryption	4	4	0
Email – client (e.g. S/MIME or Open PGP)	5	3	-2
Email – gateway (e.g. TLS)	6	7	+1
Full disk encryption	7	6	-1
Database encryption	8	8	0
Mobile device encryption	9	11	+2
Tape backup encryption	10	9	-1
USB device encryption	11	10	-1
XML encryption	12	12	0
Storage fabric / Switch encryption	13	13	0

The most significant increases in this year's research were "File encryption – server" moving up from fifth to second place and "Mobile device encryption" rising from eleventh to ninth. Email encryption at the client saw the most significant fall, from third place in 2008 to fifth in 2009. There was not a significant increase in encryption adoption for databases or backup tapes in 2009. We continue to caution organizations not encrypting these applications that they remain at serious risk of data breach – particularly with regard to patient and credit card data.

This year's research saw the addition of four new applications: 1) Network link encryption, 2) Payment processing, 3) Disk array, and 4) Cloud computing. Figure 1 and Table 2 compare the results of all respondents to those of the financial services industry, which has adopted encryption faster.

Figure 1: Encryption adoption compared to financial services industry – 2009 results

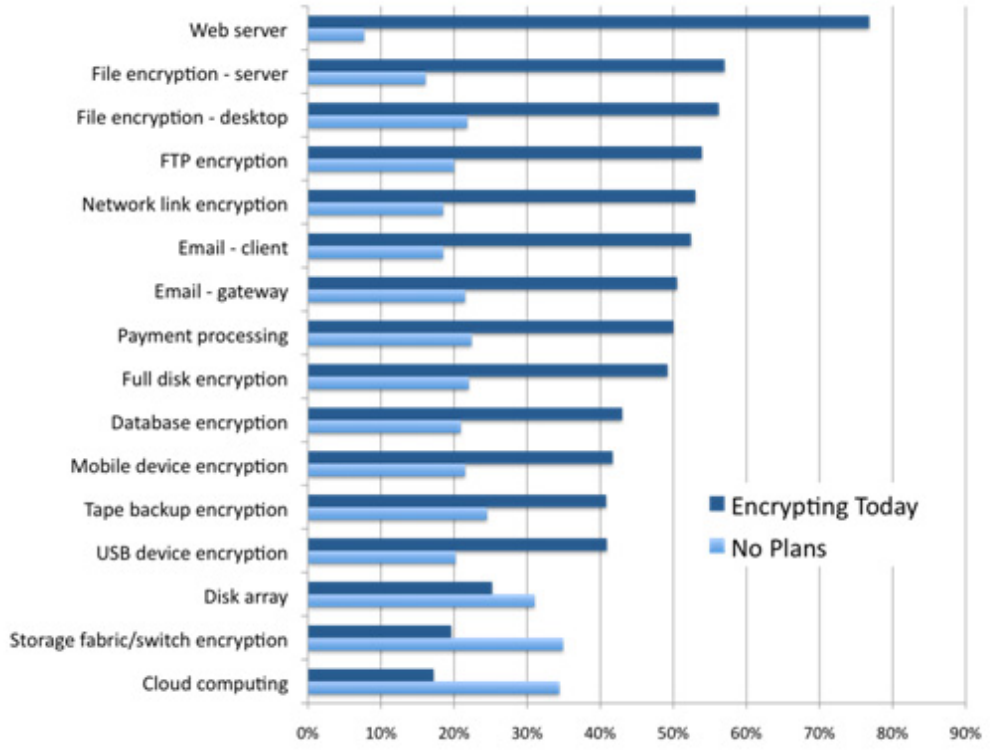


Table 2: Encryption applications used – 2009 results

Encryption application	All respondents	Financial services industry
Web server – SSL	77%	86%
File encryption – server	57%	65%
File encryption – desktop	56%	62%
FTP encryption	54%	65%
Network link encryption	53%	70%
Email – client (e.g. S/MIME or Open PGP)	52%	60%
Email – gateway (e.g. TLS)	51%	68%
Payment processing	50%	79%
Full disk encryption	49%	56%
Database encryption	43%	53%
Mobile device encryption	42%	63%
Tape backup encryption	41%	58%
USB device encryption	41%	45%
Disk array	25%	44%
XML Encryption	31%	33%
Storage fabric / Switch encryption	20%	30%
Cloud computing	17%	19%

Here we can see that the five most widely deployed encryption applications overall are:

1. Web servers (77 percent)
2. File encryption on servers (57 percent)
3. Desktop file encryption (56 percent)
4. FTP encryption (54 percent)
5. Network link encryption (53 percent)

The financial services industry differs slightly, with email encryption at the gateway and payment processing among the five most frequently used encryption applications in this year's research:

1. Web servers (87 percent)
2. Payment processing (79 percent)
3. Network link encryption (70 percent)
4. Email encryption at the gateway (68 percent)
5. Tie: File encryption at the server (65 percent) and FTP encryption (65 percent)

The financial services industry does have a higher percentage of database and backup tape encryption deployed than the general survey population. 53 percent of financial services participants encrypt databases compared with 43 percent overall. 58 percent of financial services participants encrypt backup tapes compared with 41 percent overall. Since the financial services industry has been the focal point of more data protection regulations, this trend may point toward future overall growth in database and backup tape encryption as these regulations begin to impact more industries.

We must continue to caution organizations not encrypting databases and backup tapes that they are at risk for two reasons:

1. Recent research has shown that exposing as few as 10,000 customer records can cost over $1 million in damages[1] and that the average organization pays $6 million per breach.[2]

2. Tapes and databases are transportable. Tapes are often sent outside the protected perimeter of the organization, making data vulnerable. This is also true for databases when database information is transferred, backed up to disk, or stored on tape. This means every time a backup of the database is made to tape and sent outside of the organization unencrypted, the likelihood of a data breach increases.

Obstacles to Encryption

In this year's research, we wanted to uncover more of the obstacles to encryption. Cost, availability, and key management concerns topped the list. In this section, we look at each factor separately.

[1] Gartner, "Pay for Mobile Data Encryption Upfront, or Pay More Later," November 5, 2008.

[2] Ponemon Institute, "Fourth Annual US Cost of Data Breach Study," January 2009.

Cost

Cost is still the primary issue for most organizations that want to encrypt more data where it is needed most. Table 3 shows respondents' answers to the question, "If there is data in your organization that should be encrypted but is not, what is the biggest obstacle preventing encryption?" Slightly more than half of respondents indicated the cost of either deploying or managing the solution as their biggest obstacle. Another 22 percent of participants cited data recovery costs or key management challenges as their most significant barrier.

Table 3: "If there is data in your organization that should be encrypted but is not, what is the biggest obstacle preventing encryption?"

Response	All respondents
Cost of encryption solution	**26%**
Cost of managing encryption solution	**25%**
Other	14%
Management doesn't see connection between encryption and protecting customers – thinks it's an "unnecessary expense"	13%
Cost of data recovery and key management	12%
Data recovery concerns resulting from unresolved key management challenges	10%

Data Availability

This year's research found that database and backup tape encryption are still less widely adopted than encryption for many other applications. One participant succinctly summarized the reasoning behind this reluctance: "Availability is more important than confidentiality." Others cited "ignorance," "underestimation of risks," "budget," and "neglect" as reasons why participants have not encrypted sensitive data.

Database encryption

When it comes to protecting sensitive data in databases, most think encrypting will create performance issues for business-critical applications. Even respondents from the financial services industry, with a higher rate of database encryption adoption, tend to agree. When applications process fewer transactions because of database encryption, organizations lose business. One participant told us that both performance and cost blocked their adoption of database encryption: "Poor database schema designs use sensitive data as database keys and thus drastically impacts performance. This fix is a schema redesign that most organizations are not willing to fund."

Table 4 shows participants' ideas about the main factors that have prevented organizations from deploying database encryption.

Table 4: "In your opinion, what is the main reason so many organizations are waiting to encrypt sensitive data in the database?"

Response	All respondents	Financial services industry
Creates performance impacts that may allow fewer customer transactions	**21%**	**25%**
Don't see the benefit of encrypting the database when hackers attack the front end of the applications and can get access to data whether encrypted or not	18%	19%
Key management issues are too complex	17%	18%
Requires a disruption to the application environment which may cause lost business	15%	13%
Waiting to be natively embedded in the database solution	13%	14%
Requires migrating data that will cause a disruption to the business	9%	13%
Other	7%	6%

The second most popular response came from participants who don't see the benefit of encrypting databases if they can still be attacked. Host-based attacks, SQL injection, and insider threats may not be thwarted by the use of data encryption. It's always important that a "defense in depth" approach to mitigating risks is used.

However, one of these layers should be encrypting databases. For example, if organizations back up their databases to tapes, they could be at serious risk if they ship those tapes unencrypted. Using database encryption before backing up the data can help protect sensitive information and prevent a data breach if a tape is lost or stolen.

Finally, 17 percent of participants said key management was too complex to apply encryption at the database. As we will see later in this section, many participants said they would have less than an hour to recover encrypted data from the database, creating data availability concerns. This makes effective key management that much more important.

Backup tape encryption

In regard to backup tape encryption, we asked survey respondents a similar question: "In your opinion, what is the main reason so many organizations are waiting to encrypt backup tapes?" As shown in Table 5, the most popular response was "key management issues too complex" at 24 percent. For example, one participant told us that organizations "Want to ensure access to backup tapes […] if encrypted and key is lost or unavailable then the backup tape is worthless." Others told us it was the worry about data "recoverability after long periods of storage" that discouraged encryption.

Table 5: "In your opinion, what is the main reason so many organizations are waiting to encrypt backup tapes?"	
Choices	**All Respondents**
Key management issues too complex	**24%**
Most organizations will wait until after a data breach notification event	19%
Waiting to be natively embedded in my backup tape solution	17%
Decision to postpone encrypting tapes is made by the storage dept without involvement from the security dept	11%
Encrypting tapes cost more than data breach so it's not cost-effective to encrypt	10%
Too difficult to make key accessible to the disaster recovery site	10%
"Other"	9%

Coming in second place with 19 percent was the response "most organizations would wait until after a data breach event" before they would be willing to tackle tape backup encryption. This was concerning because our assessment of the current regulatory environment concludes that organizations do not have the luxury of waiting to encrypt tapes as the likelihood of breaches and costs to the business are only increasing. In our opinion, organizations that ship tapes must encrypt tapes.

Key Management Trends

As we've seen with backup tapes and databases, key management concerns continue to plague organizations attempting to encrypt sensitive data. Once this data is encrypted, it must be recoverable at some point in the future, with little room for error. First and foremost, data must be available. Concerns around data availability have made planning an organization's key management strategy no easy feat. A third of survey respondents (34 percent) have been planning their key management strategy for over a year (up from 26 percent in 2008). Table 6 below shows how much time organizations have spent planning for key management compared to the financial services industry. Unsurprisingly, more financial services participants (47 percent) have spent over a year planning their key management strategy.

Table 6: "How much time has your organization spent preparing or planning for key management issues?"		
Length of time	**All respondents**	**Financial services**
Over 1 year	**34%**	**47%**
6–12 months	15%	19%
1–5 months	23%	16%
1 week	9%	6%
None	19%	12%

Data availability concerns are often driven by the amount of time one has to recover encrypted data. The less time to recover data, the greater the availability concerns. Table 7 below shows acceptable recovery timeframes for different applications.

Table 7: "What is an acceptable amount of time to recover data?"				
Data location	**Less than 1 hour**	**Less than 1 day**	**2 days – 1 week**	**1 month or more**
Laptops	22%	**50%**	26%	1%
Mobile devices	29%	**42%**	29%	2%
File servers	41%	**43.%**	16%	1%
Databases	**49%**	37%	13%	1%
Email	30%	**42%**	27%	1%
Backup tapes	17%	**43%**	36%	4%
Cloud computing	31%	**33%**	27%	9%
Storage fabric	30%	36%	10%	7%
Payment processing	**54%**	29%	13%	4%
Network link encryption	**54%**	30%	12%	4%

For most applications, encrypted data needs to be recovered in less than a day, but for business-critical applications like databases, network link encryption, and payment processing applications, data often must be recovered in less than an hour.

With such high demands on data recoverability timeframes, we wanted to know how encryption keys were being stored to see if there was a connection between key management and data availability requirements. Table 8 below shows the results from all survey participants and all applications.

Table 8: "Where are encryption keys stored?"					
Application	**HSM**	**Database**	**Software or disk**	**USB device**	**Don't know**
Web server – SSL	23%	13%	**29%**	9%	26%
File encryption – server	**32%**	14%	21%	5%	29%
File encryption – desktop	23%	13%	**29%**	9%	26%
FTP encryption	14%	11%	26%	4%	**46%**
Network link encryption	26%	6%	20%	3%	**45%**
Email – client (e.g. S/MIME or Open PGP)	14%	12%	31%	5%	**37%**
Email – gateway (e.g. TLS)	13%	12%	30%	4%	**42%**
Payment processing	36%	7%	13%	3%	**41%**
Full disk encryption	24%	12%	**30%**	5%	**30%**
Database encryption	24%	21%	15%	2%	**37%**
Mobile device encryption	17%	10%	23%	5%	**45%**
Tape backup encryption	26%	9%	15%	2%	**49%**
USB device encryption	14%	8%	16%	19%	**42%**
Disk array	17%	6%	12%	2%	**63%**
Storage fabric / Switch encryption	19%	5%	9%	2%	**64%**

As it was last year, the most popular response for most applications was "don't know" – even for the applications that needed to be recovered in less than an hour. However, for respondents who knew

where keys were stored, the majority of applications that needed to be recovered in an hour were most likely to be in a hardware security module (HSM). The four applications for which respondents preferred to have their keys stored in an HSM rather than software or disk were "Payment processing," "Network link encryption," "Database encryption," and "Tape backup encryption" (all highlighted in bold in the above table). Here we can see the importance of using HSMs to automate key management and overcome data availability concerns. Without HSMs or the use of automated key management tools, we believe data availability concerns will continue to stand in the way of data protection.

Conclusion

Cost isn't the only barrier to encryption adoption. The decision to encrypt requires organizations to weigh operational factors like availability and performance against the need for data protection. Here, organizations are unwilling to sacrifice operational efficiencies for data encryption. Many organizations are caught in a holding pattern while they try to determine how to best meet data recoverability requirements or find budget to meet performance and availability demands. Sadly, many will suffer a data breach before they can encrypt sensitive data. Nearly 20 percent of those surveyed believe it will take a data breach to get the approval to start encrypting backup tapes. Given the new regulatory climate, many organizations will need to ask themselves what will be worse – paying for automated encryption key management to overcome data availability fears, or losing customers in a breach when they expose sensitive credit card or patient data. Considering the higher costs and risks of a breach, we believe postponing these encryption decisions (particularly for backup tapes) is no longer a sustainable risk management strategy.

Section II: Regulations and Compliance Drivers

This year's research shows that the protection healthcare and credit card data are driving future compliance spending. This section takes a look at regulations' impact on organizations surveyed by exploring:

- Encryption budget allocated for compliance
- How survey respondents expect regulations to change
- The connection between key management and compliance

Encryption Budget Allocated for Compliance

We provided participants with a list of 25 data protection regulations and asked which ones would require the allocation of new budget in the next 24 months. Table 9 below shows the responses, with PCI DSS leading the charge, followed by US HIPAA and the EU Data Privacy Directive.

Table 9: Regulations requiring allocation of new encryption budget over next 24 months

Regulation	All respondents
PCI DSS	54%
US – HIPAA	29%
EU – Data Privacy Directive	22%
US – Gramm-Leach-Bliley	18%
US – Multiple State Data Breach Notification Laws	16%
US – California Data Breach Notification (CA SB 1386)	15%
US – Massachusetts Data Protection Act (MA 201 CMR 17)	14%
UK – Data Privacy Act	13%
US – Federal Trade Commission Red Flag Rules	12%
Canada – Personal Information Protection and Electronic Documents Act	10%
US – Nevada (Senate Bill No. 227)	9%
Canada – Privacy Breach Guideline	9%
Germany – S93 Act on Processing of Personal Data	8%
UK – Privacy Commissioner Breach Notification Guidelines	7%
South Africa – Protection of Personal Information Act	7%
Italy – Data Protection Code	4%
Spain – Personal Data Protection and Telecommunications Act	4%
Japan – Personal Information Act	4%
Hong Kong – Personal Data Privacy Ordinance	4%
Australia – Privacy Commissioner Breach Notification Guidelines	3%
France – Postal and Electronic Communications Code	3%
Australia – Commonwealth Privacy Act	3%
South Korea – Act on the Protection of Personal Information	2%
New Zealand – Privacy Commissioner Breach Notification Guidelines	2%
New Zealand – Privacy Breach Guidelines	2%

It was a surprise to see industry-driven regulations such as PCI DSS and HIPAA topping the list, given that the majority of survey respondents were not from financial services, healthcare, and retail. We believe

this indicates that encryption budget allocations are driven less by the industry you are in than by the type of data you need to protect. As more industries store, manage, and process customer, patient, employee, and business partner information, they will be required to protect their data accordingly.

Comparing the Top Five Regulations in the US and EMEA

Figure 3 and Table 10 below track the top five regulations in the US and EMEA and compare them to the worldwide response. Here you can see that while PCI DSS received the highest response in EMEA, HIPAA received the highest response in the US.

Figure 2: Percentage of respondents citing new encryption spending driven by major regulations

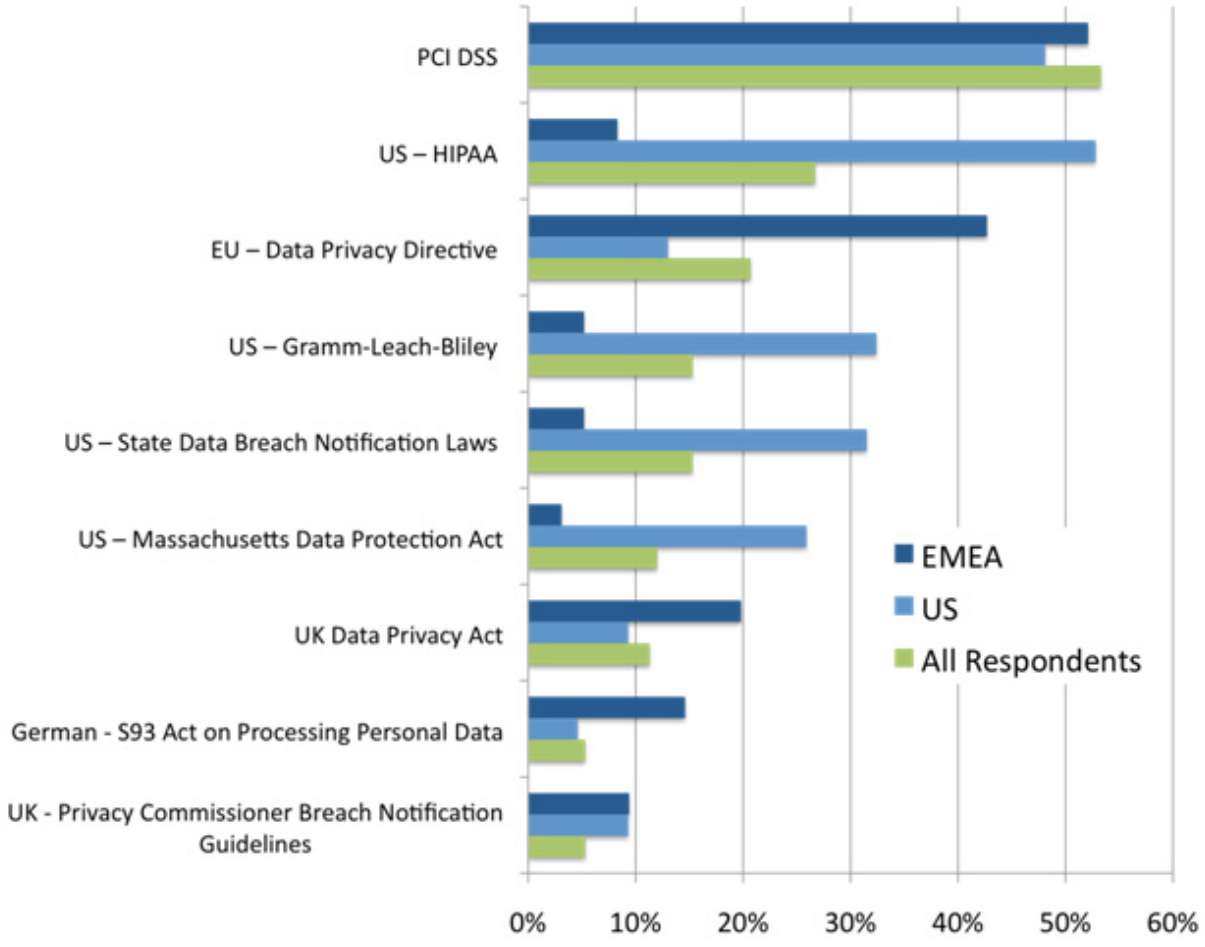


Table 10: Percentage of respondents citing new encryption spending driven by major regulations			
Regulation	**All respondents**	**US**	**EMEA**
PCI DSS	**53%**	48%	**52%**
US – HIPAA	27%	**53%**	8%
EU – Data Privacy Directive	21%	13%	43%
US – Gramm-Leach-Bliley	15%	32%	5%
US – State Data Breach Notification Laws	15%	32%	5%
US – Massachusetts Data Protection Act	12%	26%	3%
UK Data Privacy Act	11%	9%	20%
Germany - S93 Act on Processing Personal Data	5%	5%	15%
UK - Privacy Commissioner Breach Notification Guidelines	5%	9%	9%

How Survey Respondents Expect Regulations to Change

We wanted to know how participants expected regulations to change over time and if they thought regulations mandating the use of encryption were helpful or harmful to their data protection strategies.

In Figure 4 and Table 11, we asked participants how they expect regulations to change in the next 24 months. Two-thirds (66 percent) indicated they believed there would be new industry regulations, and 55 percent said they expect new national laws. Only 11 percent believed there would be no new laws introduced.

Figure 4: "How do you expect regulations to change in the next 24 months?"

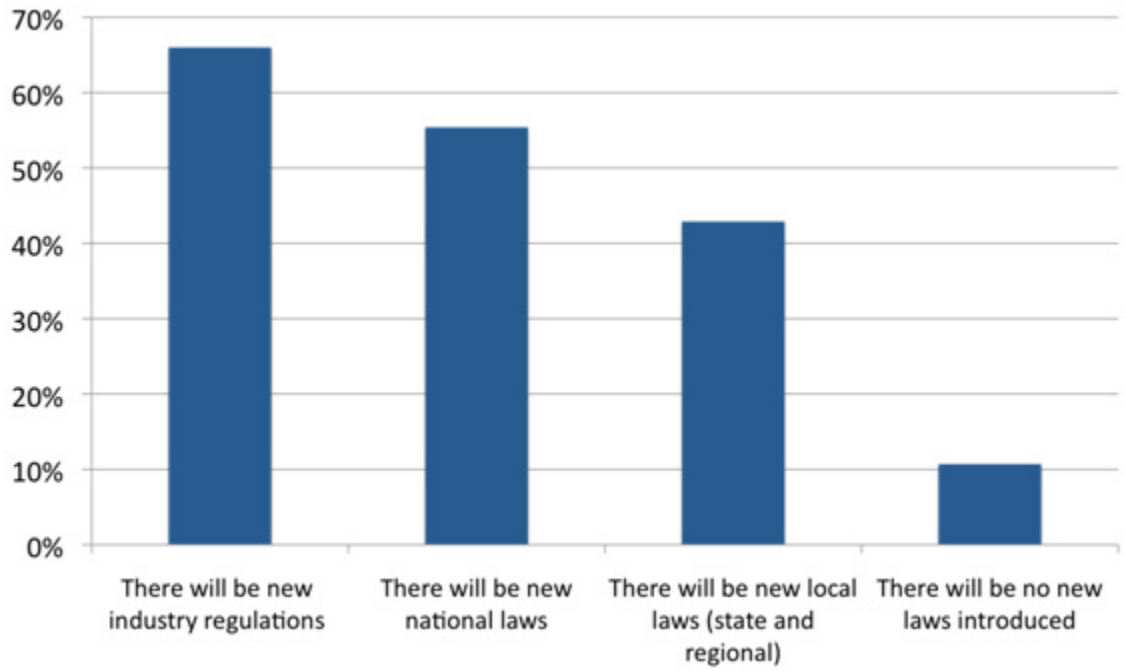


Table 11: "How do you expect regulations to change in the next 24 months?"	
Response	**All respondents**
There will be new industry regulations	66%
There will be new national laws	55%
There will be new local laws (state and regional)	43%
There will be no new laws introduced	11%

We also wanted to know how participants viewed data breach regulations that required the use of encryption. We asked them if these regulations were seen as "Helpful to moving forward your organization's data protection efforts" or "Harmful and gets in the way of your organization's data protection efforts." The overwhelming majority of respondents (70 percent) found them helpful. Surprisingly, an even higher percentage (79 percent) of respondents from organizations that have experienced a data breach found them helpful, with only 2 percent finding them "harmful."

Table 12 below compares the responses of participants whose organizations had experienced a data breach to those who had not.

Table 12: "Data breach regulations that spell out the need for protecting data using encrypting data are"		
Response	**Breached organizations**	**Non-breached organizations**
Helpful to moving forward your organization's data protection efforts	**79%**	**70%**
Undecided	19%	23%
Harmful and gets in the way of your organization's data protection efforts	2%	7%

The New Connection Between Key Management and Compliance

Over the last two years of conducting this research, we've asked participants to rank the aspects of key management they've found the most challenging. The results of this year's study highlight an interesting new finding: Organizations that have spent the most time planning key management ranked their most challenging aspect differently from their peers. Those that have been using encryption and have spent the most time preparing for key management are now more focused on demonstrating compliance compared to organizations that are just beginning to adopt encryption.

Table 13 below compares these three groups and ranks their choices from most difficult to least difficult for:

- All responses 2008
- All responses 2009
- 2009 responses by those who had spent one year or more planning key management strategy

Table 13: Relative difficulty of different aspects of key management (1=most difficult)				
	2008	2009	2009	2009 Planning Difference
Aspect of key management	All Respondents	All Respondents	1+ Year of Key Mgmt. Planning	2009 (All) to 2009 (1+ Year of Planning)
Preparing for the unfortunate publicity and impact of data breach	1	2	3	-1
Rotating keys, decrypting and re-encrypting data	2	1	2	-1
Keeping track of keys (having the right key at the right time)	3	3	7	-4
Meeting compliance requirements	4	6	4	+2
Long-term key archival	5	5	5	0
Proving compliance requirements have been met	**6**	**4**	**1**	**+3**
Making keys accessible to the disaster recovery site	7	6	6	0
Backing up and recovering keys	8	7	8	-1
Revoking/terminating keys (so data can't be accessed)	9	8	9	-1

Respondents found the following among the more challenging aspects of key management:

- Rotating, decrypting and re-encrypting data
- Preparing for the unfortunate publicity and impact of data breaches

But there were differences when it came to what was the *most* challenging. "Proving compliance requirements have been met" was ranked the most difficult by the group that had been planning key management longer. By contrast, the participants in 2008 ranked "Meeting compliance requirements" more challenging than proving they had been met. We think this is a significant finding: As organizations become more mature in their encryption and key management strategies, they find proving compliance more difficult than the mechanics of key management.

There were also interesting differences regarding the difficulty of "Keeping track of keys (having the right key at the right time)." Those who had not been planning longer than a year ranked it third in difficulty, while those who had been planning the longest found it to be one of the least challenging aspects of key management. This suggests that effective key management can reduce the time and operations costs spent on key management tasks.

Conclusion

Participants in the survey are feeling the impact of data breach regulations in two critical areas: the types of data they will need to protect and their key management strategies. While the majority of

participants worldwide are budgeting for PCI DSS, HIPAA is the most important encryption budget driver in the US. We believe this is a result of the HITECH rule introducing breach notification for sensitive healthcare data.

Second, those who have been planning their key management strategies the longest see a connection between key management and their compliance strategies. They now consider the most challenging aspect of key management to be proving that compliance requirements have been met. These organizations have more mature data protection models and are living in a compliance world where the most important aspect of data protection is their reporting capability. They are spending more time making sure their compliance efforts are demonstrable and less time deciding how and what to encrypt. Organizations that are less experienced with key management are likely dealing with newer encryption deployments and operational issues. They haven't achieved the operational efficiencies enjoyed by organizations that have been planning their key management strategies the longest.

Telephone: +1. 415. 867.8842
Contact: info@trustcatalyst.com

Section III: Cloud Computing

The security debate around cloud computing has arisen since our 2008 survey. This year, we were interested in understanding three things:

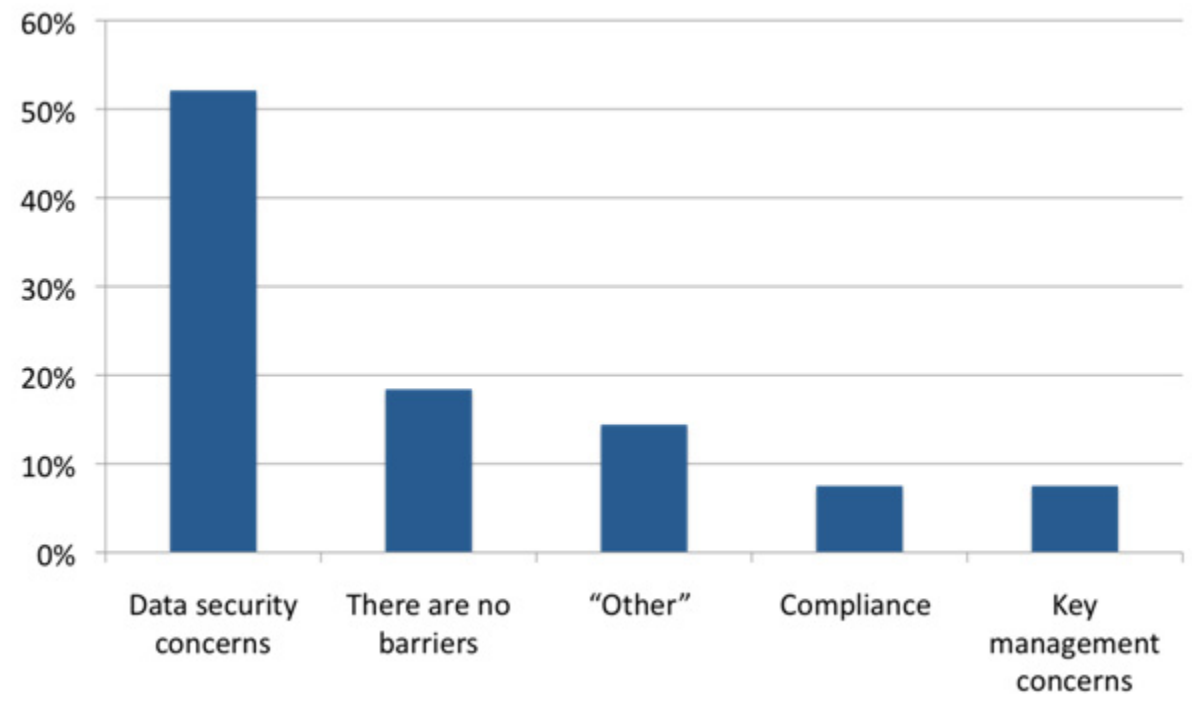
- Barriers to cloud computing adoption
- Role of encryption and data protection in an organization's decision to "move to the cloud"
- Expectations for key management with cloud computing

Figure 5 and Table 14below shows the response to the question, "What is the biggest barrier for your organization when adopting cloud computing?" 52 percent of survey participants cited data security concerns as the biggest barrier, while 18 percent said there are no barriers.

Table 14: "What is the biggest barrier for your organization when adopting cloud computing?"

Response	All respondents
Data security concerns	**52%**
There are no barriers	18%
"Other"	14%
Compliance	8%
Key management concerns	8%

Figure 3: Biggest barrier to cloud computing

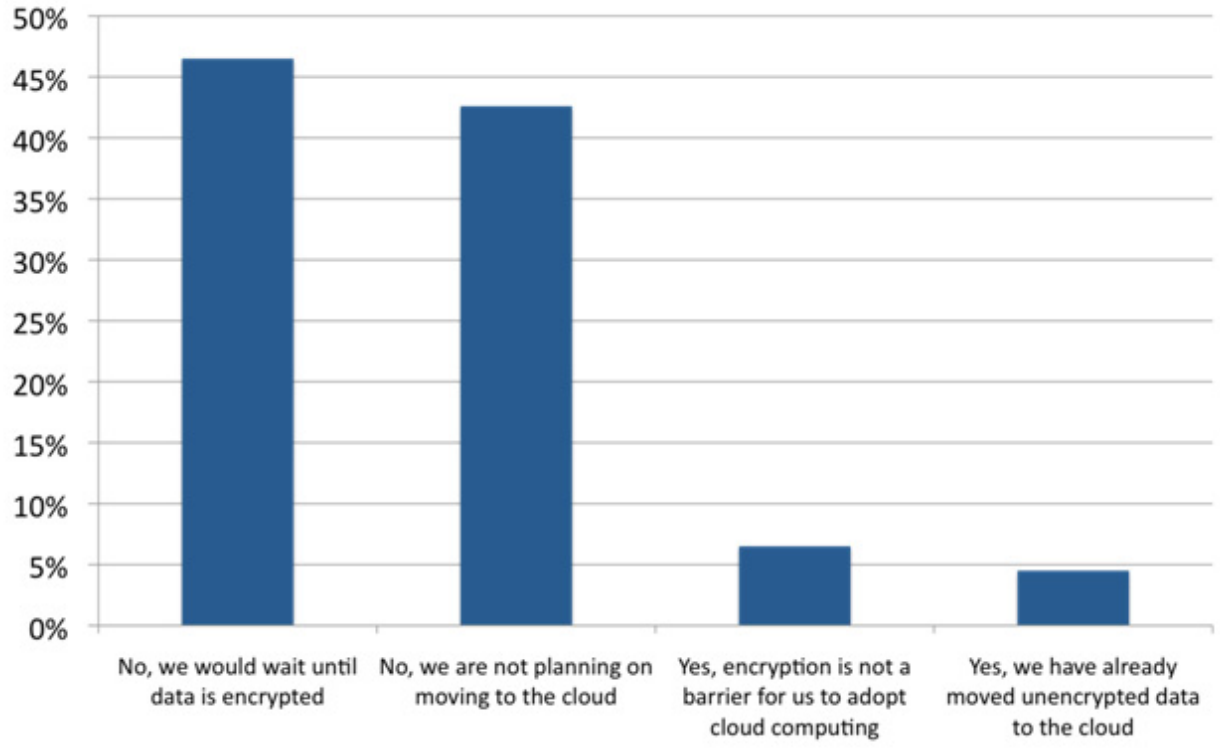


Organizations are reluctant to move to the cloud, with or without data security in place. When asked, "Would your organization move to the cloud without data encryption?", 47 percent said they would wait for encryption, but almost as many (43 percent) said they were not planning on moving to the cloud at all.

Table 15 and Figure 6 show the findings for all participants.

Table 15: "Would your organization move to the cloud without data encryption?"	
Response	**All respondents**
No, we would wait until data is encrypted	**47%**
No, we are not planning on moving to the cloud	43%
Yes, encryption is not a barrier for us to adopt cloud computing	7%
Yes, we have already moved unencrypted data to the cloud	5%

Figure 4: "Would your organization move to the cloud without data encryption?"

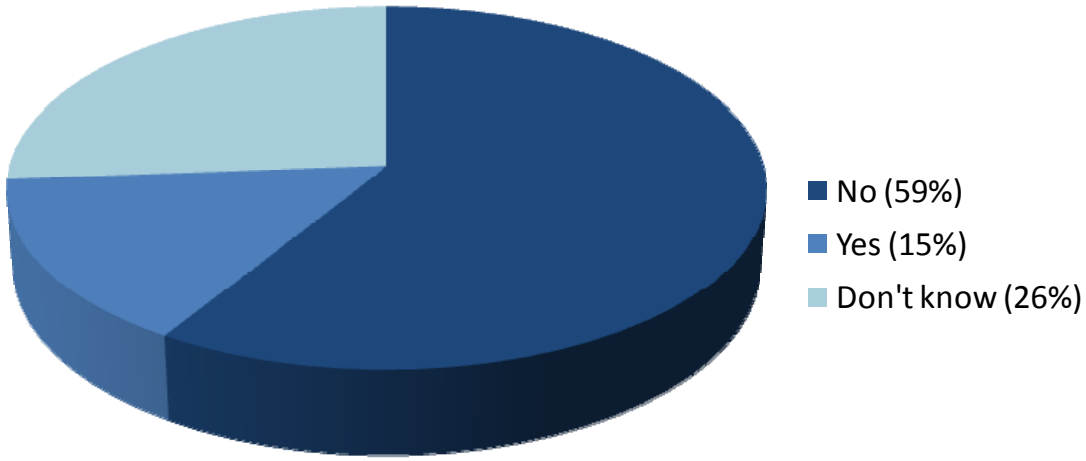


Finally, we wanted to know if encryption key management based in the cloud would be acceptable to survey participants, or if they would prefer to manage the encryption keys themselves. An overwhelming 58.8 percent said they would want to manage their own keys compared to 15.1 percent who wouldn't mind if their service provider handled key management on their behalf.

Table 16 and Figure 7 show these findings.

Table 16: "Is encryption key management based in the cloud acceptable?"	
Response	**All Respondents**
No, I would want to manage our encryption keys	59%
Yes, I trust my solution provider to manage encryption keys and recover my data in a time that is acceptable to our business	15%
Don't know	26%

Figure 5: "Is encryption key management based in the cloud acceptable?"



Conclusion

Our research shows survey respondents are very skeptical about cloud computing. While there isn't enough data here to predict any substantial trends for cloud computing, one thing is clear: Organizations should be sure to analyze whether or not a move to the cloud makes sense with a risk management framework that incorporates data protection and compliance requirements. If your organization is adopting cloud computing, then data protection, data availability, and key management expectations should be well defined in service level agreements. Organizations should also outline when they expect to be notified if breaches occur. From customers' perspective, a breach at a cloud service provider will be interpreted no differently than if you caused the breach, so be sure you and your customers are protected before using cloud services.

On the other hand, if you are a cloud computing service provider, your handling of the data protection and compliance issues covered in this report could be translated into competitive advantages in selling your services.

Telephone: +1. 415. 867.8842
Contact: info@trustcatalyst.com

Section IV: Importance of Key Management in New Data Protection Imperative

With new data protection regulations specifying encryption for safe harbor or even mandating its use, we believe it's become much riskier out there for organizations that are waiting to encrypt critical information like healthcare and credit card data in unprotected backup tapes and databases. With less than half of participants encrypting backup tapes and nearly 20 percent of respondents saying it would take the pain of a data breach to get their organization to encrypt, we believe too many organizations are needlessly at risk.

At the heart of the new data protection imperative lies a critical risk management decision. Organizations can either: 1) Wait to encrypt sensitive data and live with a much higher risk of data breach than ever before, or 2) Encrypt data but risk business continuity issues such as data availability without effective key management. The chart below summarizes this risk management decision, taking into account a few of the factors we find most important:

- **Concern:** Likelihood of a data breach versus likelihood of losing a key once data is encrypted
- **Type of notification:** What happens if your concern comes true and you have to tell others
- **Who is notified:** Exactly who is on the distribution list and alerted when things go wrong
- **Costs to business:**[3] Immediate and longer-term consequences
- **How to avoid:** Action the organization must take to avoid the problem

	Wait to Encrypt	Encrypt
Concern	Data breach	Losing keys – data availability
Type of notification	Public notification	Internal notification
Who is notified	•Customers •Employees •Shareholders •Press/Media	Staff
Costs to business	•Costs of breach •Cost of notification •Lost business •Lost customers •Fines and penalties •Litigation •Brand damage •Lost shareholder value	•Costs to encrypt/manage •Data recovery •Business disruption •Lost business
How to avoid	Encrypt data most at risk	Automate key management

[3] Please contact Trust Catalyst for the *Trust Catalyst Data Breach Prep Kit* - a cost worksheet that can help you determine costs of data breach events for your organization.

Operational efficiencies like availability and performance cause organizations to postpone implementation of their data protection strategies for fear that encryption will slow the business down (e.g., databases) or that lost encryption keys will cause lost business when data is not available (e.g., backup tapes). But we believe organizations no longer have the luxury of postponing encryption of critical data because of key management concerns. As the chart above shows, there are more costs and negative impacts to the business associated with data breaches that involve public disclosure, and most could be avoided by encrypting data.

In just the last year, we've learned a lot more about the costs of loss of customer trust after a breach. A recent survey of data breach victims[4] showed the significant impact of a breach on the business:

- 55 percent trusted the organization less, which greatly impacted future business.
- 30 percent vowed never to purchase goods from the organization again.
- 29 percent terminated future relationships with the organization.
- 69 percent of the costs of data breach came from lost business.

Our research shows, respondents were more likely to have experienced a data breach than to have lost an encryption key, as Table 17 shows.

Table 17: Incident rate for lost keys and data breaches among respondents

Event	Incident rate %
Lost key	8%
Data breach (in the last 24 months)	12%

As Table 18 below shows, for those organizations that have lost encryption keys, the event created security concerns (50 percent), resulted in permanent data loss (39 percent), and caused business disruptions (39 percent) and lost business (19 percent). While we don't want to diminish the business impacts of bad key management, we believe they can no longer serve as an excuse for postponing encryption – particularly of healthcare and credit card data.

Table 18: "What was the impact of losing encryption keys to your business?"

Response	Respondents who have lost key
Created a security concern	50%
Lost data that was never recovered	39%
Created a business disruption	39%
Lost data but we were able to recover it	31%
Caused lost business	19%
Other	4%

[4] Javelin Strategy and Research, *Consumer Survey on Data Breach Notification,* 2008.

Conclusion

We are concerned for two reasons. First, without automated key management, the encryption necessary to protect sensitive data where it is most at risk will not happen. We believe the lack of a key management strategy is no longer an acceptable reason for postponing the protection of critical data like healthcare, patient, and credit card data. The only way organizations will be able to comply with regulations and safely protect patient and consumer data will be to automate encryption key management. Technologies like HSMs (hardware security modules) have long been available to help organizations automate key management and avoid data availability issues. However, many organizations see these technologies as too costly to implement. Taking into consideration the value organizations place on availability, the operational efficiencies good key management brings, and the ability to encrypt more, we believe these technologies are well worth the cost.

Second, the costs of breach notifications are worse than we originally thought. Postponing your decision to encrypt will cost a lot more than many organizations initially estimated in their assessment of their risks. Only with automated management of keys will availability and continuity issues stop obstructing encryption projects. We believe automating key management is no longer an option – especially when it comes to protecting credit card and patient data.

Telephone: +1. 415. 867.8842
Contact: info@trustcatalyst.com

Appendix A: Research Methodology

In August 2009, Trust Catalyst conducted an online survey to examine the current and planned use of encryption and key management strategies within today's global enterprise. Prospective survey respondents were selected from a database of global information security professionals collected by Thales, a leader in the provision of information and communication systems security solutions whose customers include some of the most security-conscious organizations in the world. Over 30,000 emails were sent to information security professionals who were asked to complete the online survey. As an incentive to complete the survey, we offered the results of the survey contained within this research report. We received 655 complete and partial responses.

Respondents were given the following instructions before starting the survey:

The purpose of the survey is to gather much needed information about global market requirements in encryption and key management trends – at a level of depth and experience missing in other surveys completed to date. Like last year, the 2009 research report will be an invaluable benchmark showing how hundreds of other organizations compare to yours in the use of encryption and responding to key management challenges.

Your participation is completely confidential and all responses will be compiled at an aggregate level so your participation is completely anonymous.

Following are the demographics and organizational characteristics of the 655 respondents. Table 19 shows participants' functional responsibilities. Table 20 provides their self-reported organizational roles.

Table 19: Functional responsibilities of respondents	Percent of respondents
Compliance	5%
Database administration	1%
Information security	30%
Network security	6%
Operations	6%
PKI deployment	8%
Product / application development	14%
Risk management	4%
Storage administration / design	0.6%
System administration / design	5%
Website administration	0.3%
Other	21%

Figure 8: Functional responsibilities of respondents

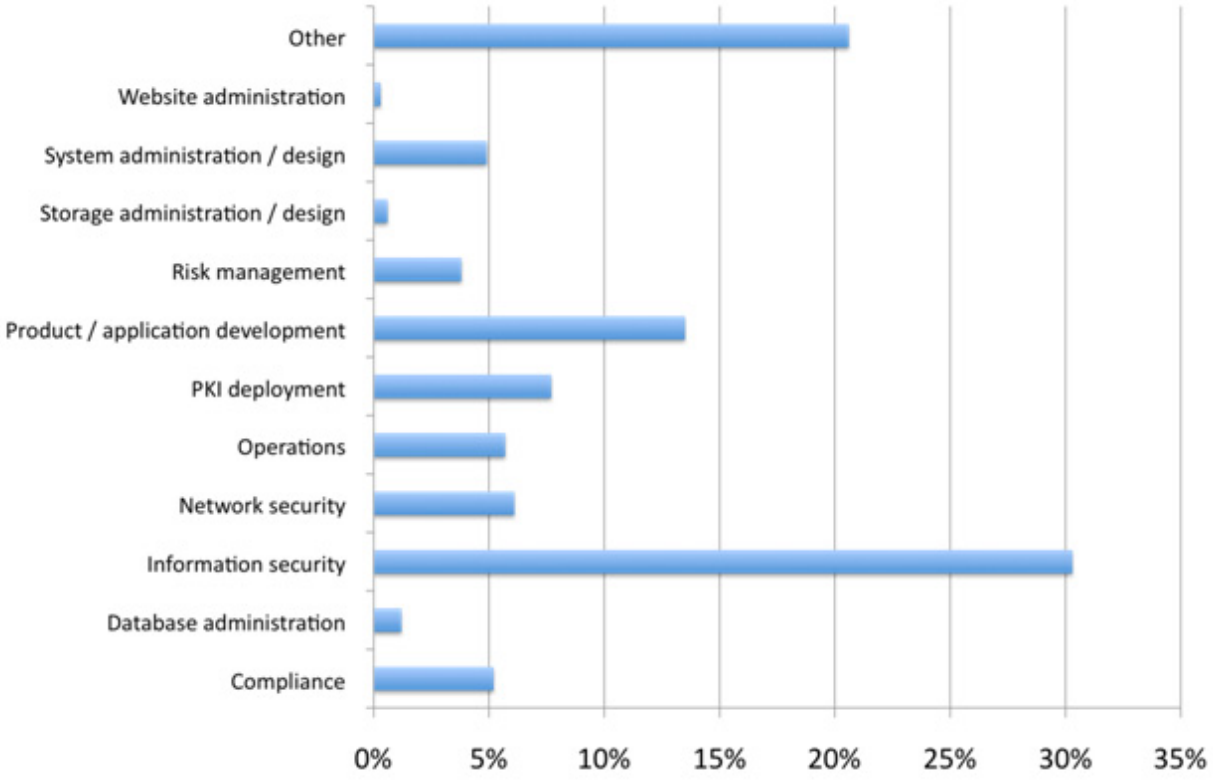


Table 20: Organizational roles of respondents	Percent of respondents
Administrator	6%
Architect	15%
Staff	8%
Manager	**24%**
Director	8%
Vice president	3%
Chief information officer	2%
Chief security officer	1%
Chief information security officer	2%
Chief compliance officer	1%
CEO	3%
Other	**27%**

Figure 9: Organizational roles of respondents

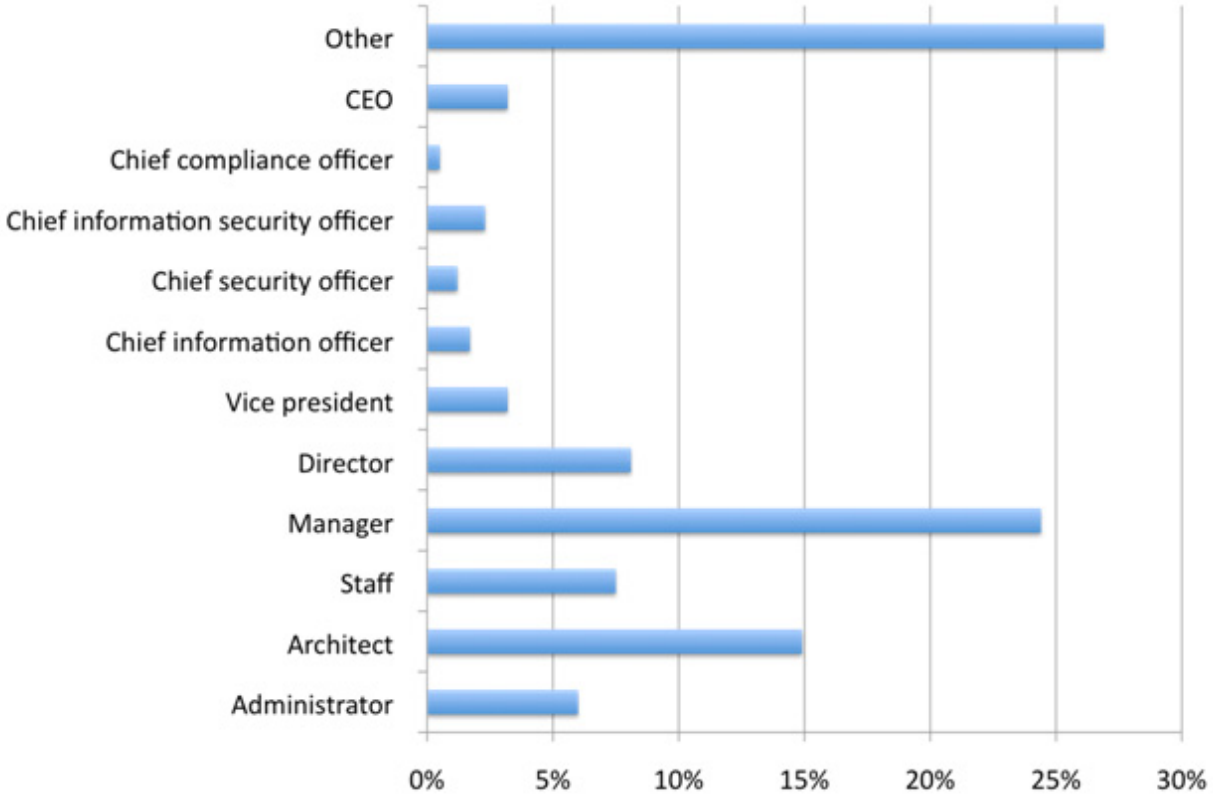


Table 21 shows the percentage distribution of survey respondents by industry classification. The two biggest industry segments were technology and software (28.5 percent) and financial services (25.7 percent).

Table 21: Industry classification of respondents	Percent of respondents
Automotive	0.3%
Defense	3%
Education	3%
Energy	1%
Financial Services	**26%**
Food services	0.3%
Government	8%
Healthcare	4%
Hospitality	0%
Internet and ISP	1%
Local Government	1%
Manufacturing	3%
Media	0.5%

Pharmaceuticals	0.2%
Professional Services	6%
Research	0.8%
Retail	2%
Technology and Software	**29%**
Telco, Wireless and Cable	3%
Transportation	0.9%
Other	8%

Figure 10 and Table 22 show the geographical breakdown of survey respondents, with the majority of respondents coming from either EMEA (Europe, the Middle East, and Africa) or the United States.

Figure 10: Location of respondents

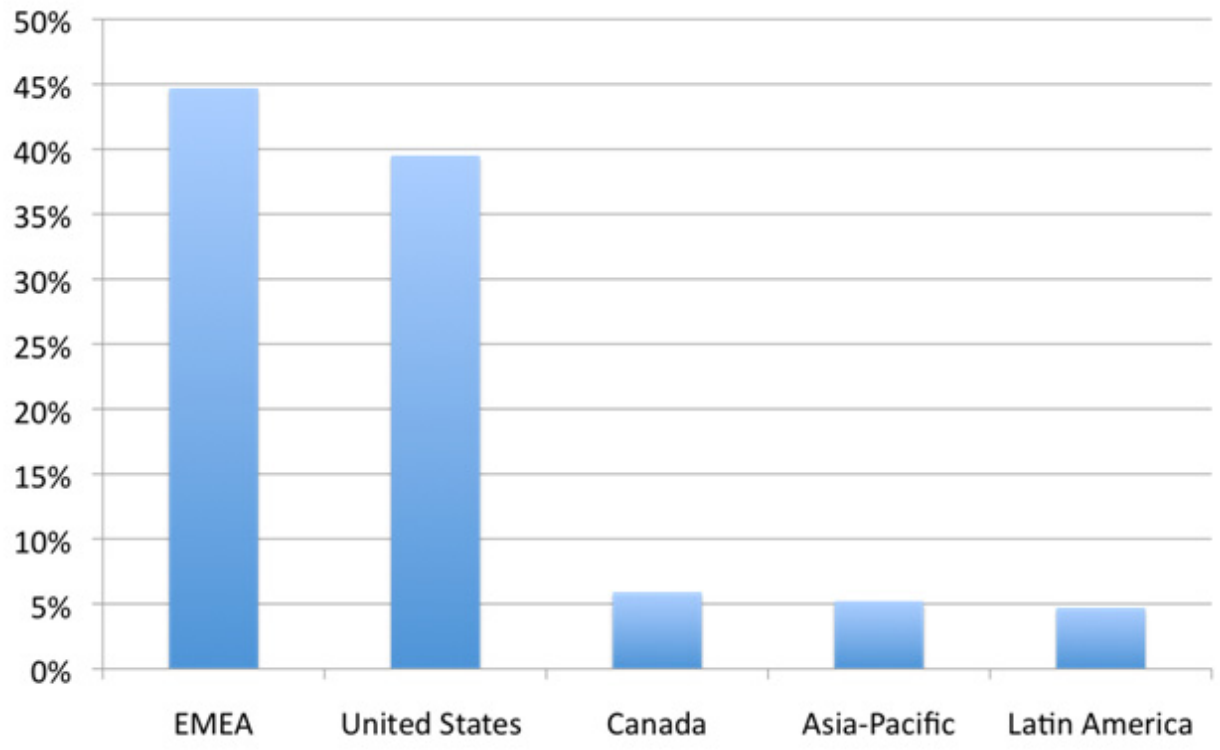
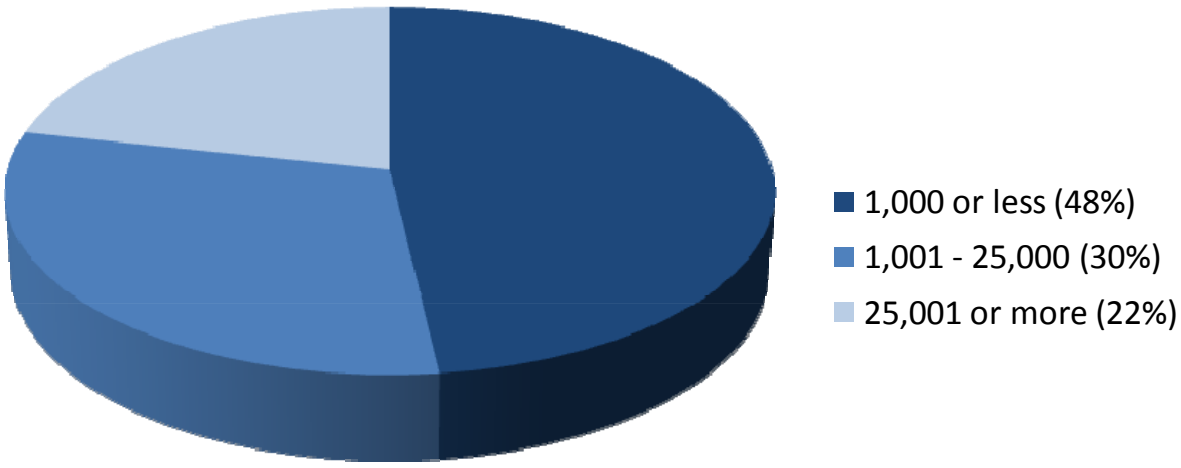


Table 22: Location of respondents	Percent of respondents
Asia-Pacific	5%
Canada	6%
EMEA	**45%**
Latin America	5%
United States	40%

Finally, respondents' company size is depicted in the figure below, with 48 percent having fewer than 1,000 employees, 30 percent having 1,001–25,000 employees and 22 percent having more than 25,000 employees.

Figure 11 Number of employees in respondent organization



About Thales

Thales is one of the world leaders in the provision of information and communication systems security solutions for government, defense, critical infrastructure operators, enterprises, and the finance industry. Thales's unique position in the market is due to its end-to-end security offering spanning the entire value chain in the security domain. The comprehensive offering includes architecture design, security and encryption product development, evaluation and certification preparation, and through-life management services.

Thales has forty years of unrivalled track record in protecting information ranging from Sensitive But Unclassified up to Top Secret, as well as a comprehensive portfolio of security products and services, which includes network security products, application security products, and secured telephony products.

About Trust Catalyst

Trust Catalyst helps global organizations make critical decisions about how to protect their most valuable resource – their customers' trust. We understand that the adoption of a successful data protection or security program is about selling a strategy to a larger audience. We speak the language business executives understand and quantify the need for security by helping establish the costs of lost customer trust, including disruption of business. As cybercriminals increasingly target organizations with sensitive customer data, we help businesses understand the threats, the costs of those threats, and how to maintain trusted relationships with customers. You can learn more and download our research at www.trustcatalyst.com.

www.trustcatalyst.com
Telephone: +1. 415. 867.8842
Contact: info@trustcatalyst.com