Sponsored by

symantec

2009 HIMSS Security Survey

sponsored by Symantec

NOVEMBER 3, 2009

HIMSS

HIMSS Foundation

2009 HIMSS Security Survey
Sponsored by Symantec
Final Report
November 3, 2009

Now in its second year, the 2009 HIMSS Security Survey, sponsored by Symantec reports the opinions of information technology (IT) and security professionals from healthcare provider organizations across the U.S. regarding key issues surrounding the tools and policies in place to secure electronic patient data at healthcare organizations. The study was designed to collect information on a multitude of topics regarding organizations' general security environment, including access to patient data, access tracking and audit logs, security in a networked environment, use of security in a networked environment and medical identity theft. This year, we have also probed our respondents with regard to their preparedness and approach for meeting new privacy and security requirements contained in The American Recovery and Reinvestment Act of 2009 (ARRA).

Contents

1. Executive Summary
2. Profile of Survey Respondents
3. General Information Security
4. Patient Data Access
5. Access Tracking/Audit Logs
6. Use and Measurement of Security Controls
7. Security in a Networked Environment
8. Use of Security Technologies
9. Medical Identity Theft
10. Conclusion
11. About HIMSS
12. About Symantec
13. How to Cite This Study
14. For More Information

Figures

All figures in this report can be found in the report Appendix; several are also highlighted throughout the report.

1. Participant Profile—Organization Type
2. Participant Profile—Title
3. Participant Profile—Region
4. Percent of IT Budget Dedicated to Information Security
5. Summary of Security Personnel
6. Frequency of Conducting a Formal Risk Analysis
7. Components of a Formal Risk Analysis
8. Uses for Risk Analysis Data
9. Length of Time Needed to Correct Deficiencies in Security Controls and Policies
10. Tracking Access to Electronic Patient Information
11. Access of Electronic Data by Patients/Surrogates
12. Types of Data Patients/Surrogates can Access
13. Types of Systems from Which Data is Collected and Analyzed
14. Methods for Analyzing Log Information
15. Events Captured by Audit Logs
16. Use of Audit Log Data
17. Accounting Disclosure of Patients
18. Plan in Place to Respond to Threats or Security Breaches
19. Active Determination of Cause/Origin of Security Breach
20. Means for Monitoring Success of Security Controls in Place
21. Means for Measuring Success of Security Controls in Place
22. Existing Data Sharing Relationships
23. Data Sharing Requirements That Necessitate the Use of Additional Security Tools
24. Does Organization Evaluate Risk of Medical Identity Theft as Part of Privacy/Security Profile
25. Instances of Medical Identity Theft at Your Organization
26. Experienced Any Consequences from a Case of Medical Identity Theft
27. Change in Business Practice at Organization

1. Executive Summary

Results from the 2009 HIMSS Security Survey, sponsored by Symantec, suggest that, despite changes to the security and privacy landscape including new legal and regulatory requirements and increasing risk, healthcare organizations have made relatively little change since the assessment of the market HIMSS conducted in 2008 across a number of important areas of the security environment. This is reflected in the assessment of 196 IT and security professionals of their own organization's readiness for today's risks and security challenges. Respondents characterized their own maturity level as mid-range, budgets dedicated to security remain low, and many organizations still do not have a formally designated CSO/CISO. Also, organizations often do not have a plan for responding to threats or incidents relating to a security breach.

Furthermore, risk assessments are not universal among the responding organizations – only three-quarters perform such an assessment. Importantly, of those organizations that do actively perform risk assessments, almost three quarters indicated that patient data at their organization was found to be at risk as a result of inadequate security controls, policies and/or procedures. The risk assessment activity positions organizations to correct deficiencies and the survey data serves to emphasize the important role and value that ongoing security risk analysis can play in protecting health data.

The survey also assessed some aspects of healthcare organizations' readiness to comply with the new privacy statutes in American Recovery and Reinvestment Act of 2009 (ARRA). Results also showed that audit logs are widely used among the healthcare organizations represented in this survey. Data from firewalls, application logs and server logs are common sources of information retained in the audit logs. However, at this time, only one-quarter of respondents reported that analysis of log data is done entirely electronically. Without the assistance of some automated/electronic means to analyze log data, organizations may not be well positioned to provide patients with a breach notification. In addition, they may have difficulty producing a clear and accurate accounting of disclosures. Finally, while tools such as firewalls and user access controls are widely used, many organizations are not using all available technologies to secure data, such as encryption to secure data in transmission (which is used by just 67 percent of responding organizations) and fewer than half encrypt stored data.

Healthcare organizations today face increasing challenges as they are being urged to adopt electronic health records in the midst of a complex legal, regulatory and risk environment. To effectively secure patient data, it is important that organizations appropriately resource and manage their security initiatives. Trends as reflected in the survey results indicate that organizations are currently required to be extremely efficient in terms of how they are using their resources. These factors will become even more critical factors in the future, as organizations will have to continue to deal with an increasingly complex operating environment.

Key survey results include:

Maturity of Environment: Respondents characterized their environment at a middle rate of maturity, with an average score of 4.27 on a scale of one to seven, where one is not at all mature and seven is a high level of maturity.

Security Budget: Approximately sixty percent of respondents reported that their organization spends three percent or less of their organization's IT budget on information security. This is consistent to the level of spending identified in the 2008 study, and indicates that little additional resources have been applied to information security.

Formal Security Position: Fewer than half of respondents indicated that their organization has either a formally designated CISO (Chief Information Security Officer) or CSO (Chief Security Officer).

Risk Analysis: Three-quarters of surveyed organizations conduct a formal risk analysis (only half of these conduct this assessment on a yearly basis or more frequently), which has remained the same in the past year. Three-quarters of organizations that did conduct risk assessments found patient data at risk due to inadequate security controls, policies and processes. Conducting this analysis positions organizations to identify gaps in their security controls and/or policies and procedures.

Security Controls: Most respondents reported that they use the information generated in their risk analysis to determine which security controls should be used at their organization. About 85 percent of respondents reported that they *monitor* the success of these controls and two-thirds of these respondents *measure* the success of these reports.

Patient Data Access: Surveyed organizations most widely use user-based and role-based controls to secure electronic patient information. Approximately half of respondents reported that their organization allows patients/surrogates to access electronic patient information. Patients/surrogates are most likely to be granted access to high level clinical information, such as diagnosis or lab results.

Management of Security Environment: Nearly all respondents reported that their organization actively works to determine the cause/origin of security breaches. However, only half have a plan in place for responding to threats or incidents related to a security breach.

Security in a Networked Environment: Nearly all respondents reported that their organizations share patient data in an electronic format. Respondents were most likely to report that they share data with state government entities. Respondents also reported that the area in which they are most likely to share data in the future is with Health Information Exchanges (HIEs)/Regional Health Information Organizations (RHIOs). Approximately half of these organizations (41 percent) indicated that these sharing arrangements have resulted in the use of additional security controls beyond those that were already in place at their organization. This is similar the data reported in the 2008 survey.

Future Use of Security Technologies: E-mail encryption and single sign on and were most frequently identified by respondents as technologies that were not presently installed at their organization but were planned for future installation.

Medical Identity Theft: One-third of respondents reported that their organization has had at least one known case of medical identity theft at their organization. However, only a handful of these organizations experienced direct consequences from the breach.

2. Profile of Survey Respondents

A total of 196 responses were received for this survey. Data was collected via a web-based survey between August 21, 2009 and October 5, 2009. The 2008 survey had 155 respondents.

Nearly three-quarters of respondents indicated that they are a senior Information Technology (IT) executive at their organization. Specifically, 56 percent of respondents indicated that they are the Chief Information Officer at their organization. Another eight percent are Vice President of IT/IS. A similar percent reported that their title is Director of IS. Approximately 17 percent of respondents reported their title to be Chief Security Officer and two percent indicated their title is Chief Privacy Officer. The remaining ten percent of respondents reported their title as "other", which includes a wide variety of IT and security titles. See Figure One below.

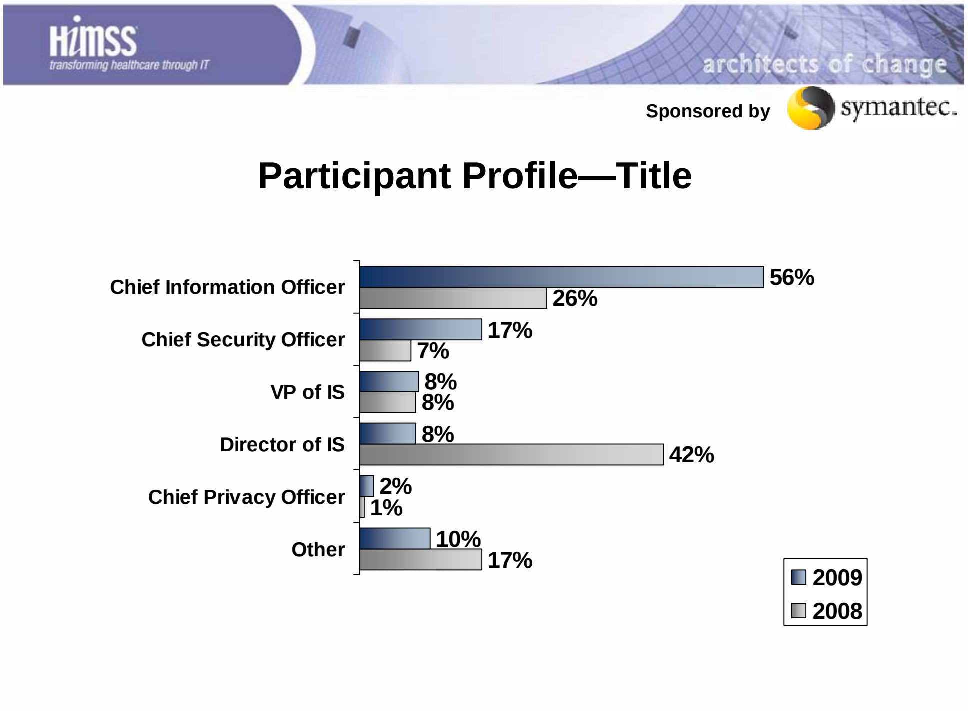
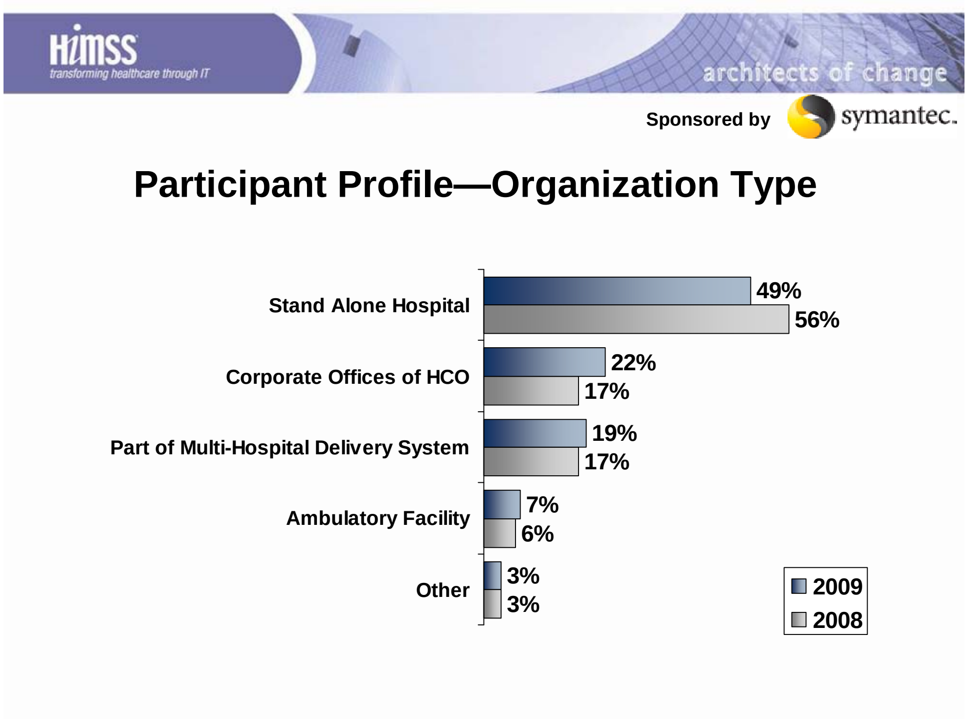


Figure One. Participant Profile—Title

Nearly half of the survey respondents reported that they work for a stand-alone hospital. Another 22 percent work at the corporate offices of their healthcare organization and 19 percent work for a hospital that is part of a delivery system. Seven percent work for an ambulatory facility. The remaining respondents work for a variety of healthcare organizations, including payers and home health agencies. See Figure Two.



Participant Profile—Organization Type

Figure Two. Participant Profile—Organization Type

Nineteen (19) percent of respondents came from the East North Central region. This is followed by the West North Central (15 percent), South Atlantic (12 percent), Pacific (11 percent) and Middle Atlantic or New England (1o percent each). The smallest number of respondents comes from the East South Central region (seven percent).

Finally, nearly one-quarter (21 percent) stated that they spent less than one percent of their budget on information security. Another forty percent reported that their organization spends between one and three percent of their budget on information security. One-quarter spend between four and six percent of their budget on information security. See Figure Three.

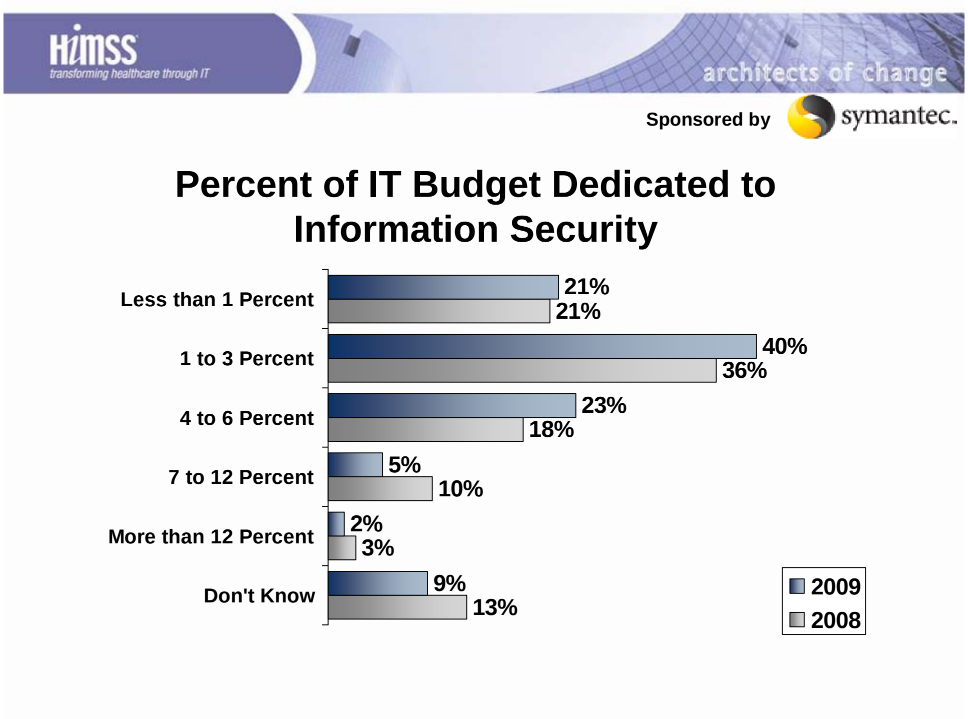


Figure Three. Percent of IT Budget Dedicated to Information Security

3. General Information Security

Fewer than half of survey respondents indicated that their organization has a formally designated Chief Information Security Officer or Chief Security Officer. Despite this, nearly three quarters conduct a formal risk analysis. About half of the respondents indicated that this risk analysis is conducted at least annually. The result of this risk analysis was that about organizations were able to identify gaps in either their organization's security controls or their policies and procedures that posed a serious or significant threat to patient information.

Survey respondents were asked to identify whether or not their organization has either a formally designated CISO (Chief Information Security Officer) or CSO (Chief Security Officer). More than half of survey respondents (58 percent) indicated that their organization did NOT have an individual with this title employed at their organization. Conversely, only two percent indicated that they have both a CISO and a CSO. The remaining respondents have either a CISO (22 percent) or a CSO (19 percent). This question was not asked in the 2008 survey.

Respondents were also asked to identify how frequently their organization conducts a formal risk analysis to evaluate risks to patient data at their organization. About three-quarters of respondents (74 percent) reported that their organization does conduct a formal risk analysis. This is comparable to the 78 percent that reported this to be the case in the 2008 survey. Among those respondents that reported their organization conducts a formal risk analysis, nearly half (47 percent) reported that this risk analysis is conducted on an annual basis, with another eight percent reporting that their organization conducts a risk analysis at least every six months. Another (26 percent) reported that this analysis is conducted once every two years. One percent of respondents did not know how frequently this type of analysis was conducted. These numbers are comparable to those reported in the 2008 survey. See Figure Four.

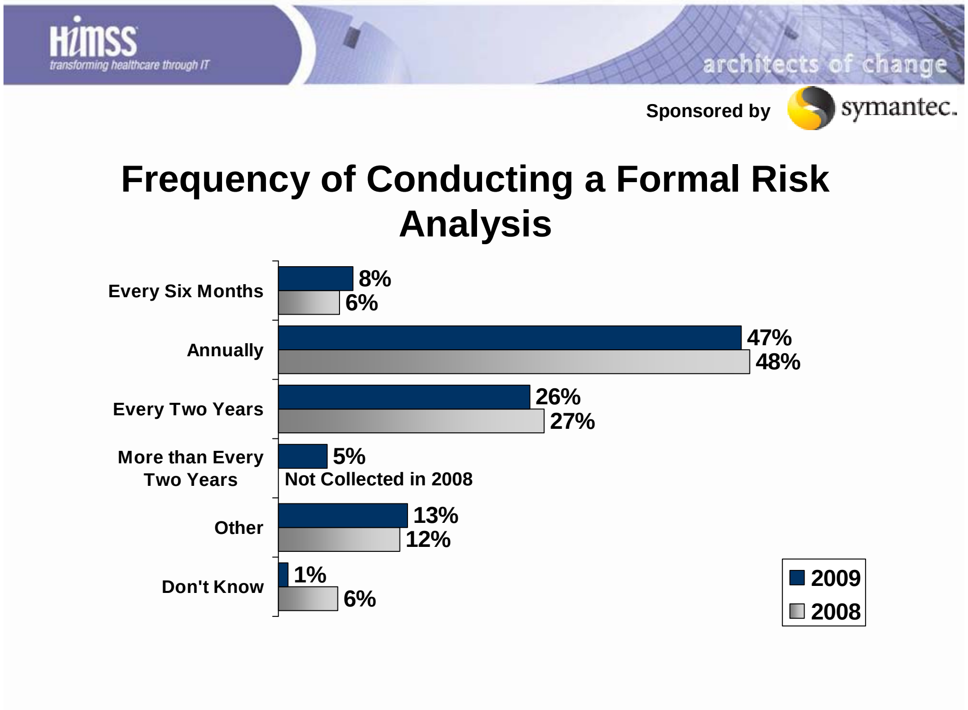


Figure Four. Figure of Conducting a Formal Risk Analysis

Among those that conduct a risk analysis on a formal basis, nearly all (94 percent) reported that their organization includes an analysis of external threats in their risk assessment. This was also the most frequently identified component of a risk analysis in the 2008 research. A similar number of respondents (91 percent) indicated that they include internal threats as part of their risk assessment. This was the same percent of respondents that indicated that their risk assessment includes an evaluation of risks to the confidentiality of patient data. The frequency with which the other responses for this question were selected are listed below.

- Compliance requirements (88 percent);
- Evaluation of the adequacy of your organizations policies/procedures (83 percent);
- Evaluation of the effectiveness of your organization's security controls (83 percent);
- Risks to the availability of patient data (74 percent);
- Risks to the integrity of patient data (72 percent).

The only area not identified by three-quarters of respondents was evaluation of new opportunities to cost-effectively improve security. This option was selected by 42 percent of respondents. These percentages are all consistent with what was reported in the 2008 survey.

The result of this risk analysis was that about organizations were able to identify gaps in either their organization's security controls or their policies and procedures that posed a serious or significant threat to patient information. While 22 percent of respondents indicated that they did NOT identify a serious threat to patient data, half (52 percent) indicated that patient data at their organization was at risk as a result of both a lack of effective security controls and a lack of adequate policies and/or procedures. Another 15 percent indicated that their organization's patient data was at risk as a result of a lack of effective security controls in place at their organization and five percent indicated that their organization's patient data was at risk because their organization did not have adequate policies and procedures in place.

Respondents were also asked how long it took to correct the deficiency in security tools and policies in procedures that were deemed inadequate in the risk analysis. One-third of respondents indicated that it took them less than six months to correct their identified deficiency in security controls; another 40 percent said that it took six months to one year. However, eight percent of respondents indicated that this deficiency has not been corrected. With regard to the length of time it took to correct a deficiency in policies and/or procedures, nearly half said that it took then less than six months to resolve the issue. Another third (34 percent) noted that it took them between six and 12 months to resolve the issue. Only one percent of respondents noted that this issue has still not been corrected.

At present, on a scale of one to seven, where one is not at all mature and seven is very mature, respondents rated the maturity of their systems as a 4.27. Indeed, nearly half of respondents rated their maturity as a four or a five, with very few respondents choosing the outer limits of the scale. A score of one was identified by only three percent of respondents and a score of seven was identified by only four percent of respondents.

4. Patient Data Access

All of the individuals responding to this survey reported that their organization has mechanisms in place to monitor how their employees are accessing electronic patient information. User-based and role-based controls are most widely used. Approximately half of respondents reported that their organization allows patients and/or their surrogates to access information in an electronic format.

Respondents were asked to identify how their organizations controlled employee access to electronic patient information. Indeed, all organizations that maintain electronic patient information also reported that they use at least one method for controlling access to electronic patient information, such as user-based, role-based or rule-based access. This is consistent to what was reported in 2008. Approximately 41 percent of respondents reported that their organization uses only one method of controlling access and another 27 percent reported that their organization uses two methods of control. The remaining respondents reported that they use three or more methods of controlling access to data.

Three-quarters of respondents (76 percent) indicated that they used role-based controls to limit employee access to patient data. For the purposes of this research, role-based controls are defined as a person being able to access patient information based on their job type, such as clinician or nurse. A similar number of respondents indicated that their organization limits access to patient data using user-based controls, which limits access to data based on a person's specific identity. This item was selected by 70 percent of respondents. In fact, all respondents but three reported that at least one of these access control measure was in place at their organization. These options were the top options selected in the 2008 survey.

Other means of controlling access to patient data include group-based access, location-based access and rule-based access. Approximately one-quarter of respondents (28 percent) indicated that access to patient data was restricted by group, whereby access is limited to a specific group of people, such as all nurses who see patients in the ICU. Another quarter (23 percent) reported that they use location-based access, which was defined in this research as those who work on a particular floor or unit. A smaller percentage (eight percent) use rule-based access, which limits access using an if/then statement.

Approximately half of respondents reported that their organization permits the sharing of electronic data with patients and/or surrogates. This is nearly twice the number that reported this to be the case in the 2008 survey. Half those respondents that reported that their organization permits this type of access indicated that their organization shares high level information, such as diagnosis or lab results. Another 44 percent indicated that patients and/or surrogates could access financial/insurance information, such as a summary of the patient's account. Slightly more than one-third of respondents (37 percent) indicated that patients and/or surrogates could access scheduling information. Finally, 33 percent of respondents indicated that patient and/or surrogates could access detailed clinical information, such as summary notes prepared by a clinician. This is the only area in which the numbers have increased in comparison to 2008 data.

Finally, respondents were asked to identify if their organization had implemented security controls on the health website/portal that was offered to patients. Nearly half indicated this was the case.

5. Access Tracking/Audit Logs

Audit logs are widely used among the healthcare organizations represented in this survey. Data from firewalls, application logs and server logs are common sources of information. At this time, most respondents reported that they analyze some, if not all of the information in these logs through manual means. Approximately one-quarter reported that all analysis is done electronically.

Most respondents (94 percent) reported that their organization collects and analyzes information in the audit log; this is slightly higher than the 90 percent that reported this to be the case in the 2008 survey. More than 80 percent of the respondents collecting and analyzing information in an audit log reported that the firewall log is a source of information that is reviewed (83 percent). Three-quarters of respondents also reported that they collect and analyze information from their applications and 70 percent collect and analyze information from their servers. Nearly this many (69 percent) also collect and analyze the logs from their intrusion detection system. Respondents were least likely to collect and analyze information from their additional storage devices (15 percent) or use a data reduction/analysis tool (ten percent). A full list of systems from which respondents collect and analyze data is listed below. See Figure Five.

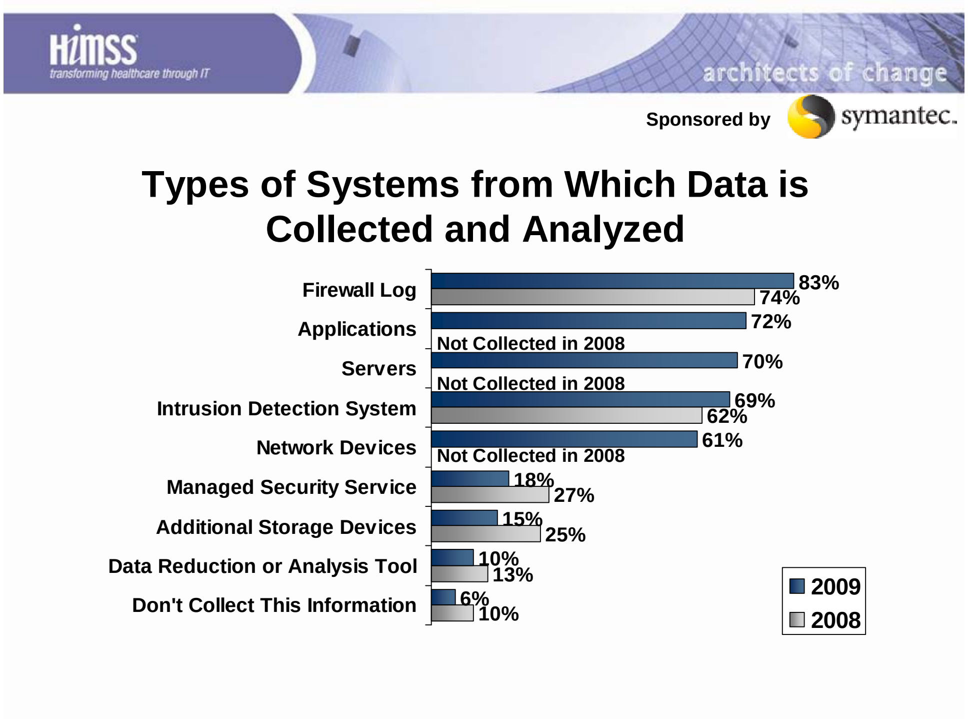


Figure Five. Types of Systems from Which Data is Collected and Analyzed

With respect to the manner in which information from the audit logs is analyzed, approximately 38 percent reported that the information was analyzed only via a manual process. Another 36 percent indicated that they used a combination of manual and other means, such as a Syslog server or log management appliance to analyze the information. Slightly more than one quarter (26 percent) reported that their organization audited information only using automated process. This is consistent with the data that was reported in 2008.

The data above clearly suggests that manual processes are widespread and nearly three-quarters of respondents use this method for collecting and analyzing log information. With regard to the automated methods in place for collecting and analyzing log information, slightly more than one-third of respondents (37 percent) reported that they use a Syslog server. Log management appliances were used by approximately 27 percent of respondents and organic application log management capabilities were used by 18 percent of respondents. The percentages for automated processes are similar to those reported in 2008.

Respondents were also asked to identify the types of events their audit log captures. Most frequently identified was security-critical events only, such as the use of authorization mechanisms like passwords (81 percent). This is followed by clinician access to data, which was identified by 72 percent of respondents. Two-thirds (64 percent) indicated that their audit log captures information on non-clinician access to data. Only 12 percent noted that their audit log captures information on patient access to data. This presents a different picture than was identified in the 2008 survey, when clinician access to data, which is captured at 79 percent of respondents' organizations, was the top response, followed by non-clinician access to data, which was identified by 77 percent of respondents. This year's most frequently selected response, security critical events, was chosen by 68 percent of respondents in the 2008 survey.

Approximately three-quarters of respondents (72 percent) reported that their organization actively uses audit log information for intrusion detection. Two-thirds of respondents (69 percent) use their audit log information for monitoring compliance with their corporate policy. A similar percent (68 percent) also indicated that they actively use audit log information for system activity monitoring. Conversely, fewer than half (44 percent) actively use their audit log information to provide accounting of disclosures to patients. All of these items were selected by fewer respondents this year than in the 2008 survey.

Among the respondents who indicated that their organization provides an Accounting of Disclosures to patients, 46 percent reported that the audit log is the primary source of information from which they get this information.

Finally, while nearly all respondents (93 percent) indicated that their organization actively works to determine the cause/origin of a security breach only about half of respondents reported that their organization has a plan in place for responding to threats or incidents relating to a security breach. Another 41 percent report that their organization is currently putting this plan together; six percent of respondents reported that their organization has no plan in place and does not intend to develop a plan.

6. Use and Measurement of Security Controls

Survey respondents were likely to report that their organization uses information generated in their risk assessment to identify which security controls to put into place. Two-thirds of respondents indicated that the success of these security controls was measured using items such as reduced risk of exposure and number of detected security incidents.

A high percentage of respondents that conducted a risk analysis (83 percent) indicated that they used the information generated by their risk analysis to determine which security controls to put into place. This can be compared to 81 percent of 2008 respondents.

Virtually all of the respondents (98 percent) reported that have security controls in place and 87 percent *monitor* the success of these controls. This is a slight decrease from the 93 percent of respondents that indicated that they monitored their security controls in the 2008 study. Approximately half of these respondents (48 percent) reported that their organization monitors the success of the security controls by conducting an external risk analysis/vulnerability analysis/penetration testing. A similar percent (46 percent) reported that they monitor this by conducting an internal risk analysis. Approximately 42 percent noted that they conduct an external compliance audit.

About two thirds of respondents (61 percent) of respondents that monitor the success of their security controls also *measure* the success of these controls. This is somewhat decreased from the three-quarters of respondents who reported this to be the case in 2008. The most frequently used measure is identifying the number of detected security incidents; this was selected by 70 percent of respondents. Slightly more than half (57 percent) indicated that their organization measures success by evaluating the reduced risk exposure that their organization experiences as a result of use of these controls. Only eight percent reported that their organization measures the return on investment that they get from the cost of tools when compared to the risk reduction. All of these numbers are less than reported in 2008.

7. Security in a Networked Environment

Nearly all respondents reported that their organization shares patient data in an electronic format. Data is most frequently shared with state government, third party providers and other facilities within the corporate organization.

Respondents were asked to identify the types of organizations with which they share patient data in electronic format. Approximately 91 percent of respondents reported that their organization shares information with at least one other type of organization. This is similar to the 94 percent of respondents who reported this to be the case in the 2008 study. The percentage of respondents sharing information with different types of organizations is identified in the table below. Figure Six.

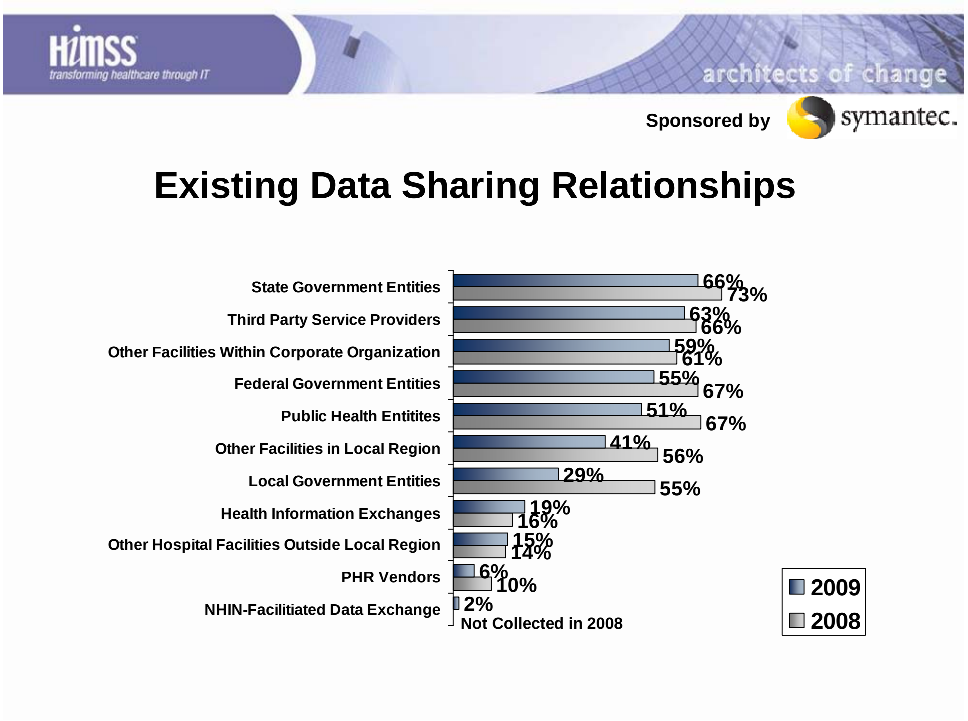


Figure Six. Existing Data Sharing Relationships.

There is also a substantial amount of activity surrounding *future* plans for sharing electronic data. These items are outlined below:

- Health information exchanges – 60 percent;
- Other hospitals/facilities within my local region that are not part of our corporate organization – 47 percent;
- Other hospitals/facilities outside of my local region/state – 40 percent;
- PHR vendors – 38 percent;
- NHIN-facilitated data exchange – 34 percent;
- Public health entities – 27 percent;
- Other hospitals/facilities within my corporate organization – 26 percent;
- Local government entities – 24 percent;
- Federal government entities – 24 percent;
- State government entities – 22 percent;

- Third party services/vendors – 19 percent;

Slightly fewer than half of these respondents (41 percent) indicated that their current data sharing arrangements have resulted in the use of additional security controls beyond those that were already in place at their organization.

8. Use of Security Technologies

Firewalls and user access controls have reached a level of saturation in the market. In general, satisfaction with the existing security technologies in place in their organizations is high among respondents. Among survey respondents, e-mail encryption and single sign-on were the technologies that are most likely to be considered for future use.

Respondents were asked to identify the types of security tools that are in place at their organization. Nearly all respondents report that a firewall is in place and 94 percent indicated that user access controls have been established. Utilization of the remaining technologies in this survey are listed below:

- Audit logs of each access to patient health records – 83 percent;
- Wireless security protocols – 82 percent;
- Off-site storage – 83 percent;
- Disaster recovery – 78 percent;
- Electronic signature – 69 percent;
- Data encryption (data in transmission) – 67 percent;
- Intrusion prevention/detection service – 66 percent;
- E-mail encryption – 60 percent;
- Data encryption (data in storage) – 44 percent;
- Mobile device encryption – 39 percent;
- Network encryption – 35 percent;
- Two-factor authentication – 33 percent;
- Single sign on – 29 percent;
- Public key infrastructure – 26 percent;
- Data loss prevention – 24 percent;
- Biometric technologies – 19 percent;
- E-discovery – 13 percent.

Among the technologies that at least half of the respondents are using, satisfaction is highest for firewalls (6.37) and wireless security protocols (6.21)[1]. Firewalls and wireless security protocols were the top tools with which users were satisfied in the 2008 survey. Data encryption for data in transmission and off site storage were the only other items with a satisfaction level of over six, with scores of 6.13 and 6.01 respectively. Satisfaction levels for the other technologies used in at least half of respondents' organizations are also high, with averages of more than five. A list of the remaining technologies is provided below.

- Mobile device encryption – 5.99
- Network encryption – 5.98
- Data encryption (data in storage) – 5.96

[1] This is based on a one to seven scale, where one is not at all successful and seven is very successful.

- Intrusion prevention/detection service – 5.84
- Single sign on – 5.80
- E-mail encryption – 5.77
- Electronic signature – 5.72
- User access controls – 5.70
- Public key infrastructure – 5.59
- Data loss prevention – 5.59
- eDiscovery – 5.59
- Biometric technologies – 5.58
- Disaster recovery – 5.41
- Audit logs – 5.30

More than half of the survey respondents noted that their organization plans to purchase e-mail encryption technology and 41 percent noted plans to purchase single sign-on technology. These were also the top technologies that respondents indicated they would purchase in the 2008 survey. Other technologies that at least one-quarter of respondents plan to purchase include mobile device encryption (32 percent), data loss prevention (28 percent) and data encryption for stored data (27 percent).

Biometric and e-discovery technologies, which are both currently used by less than 20 percent of respondents' organizations do not have high levels of projected future use, at 18 and 22 percent respectively.

9. Security Breaches and Medical Identity Theft

One-third of respondents (32 percent) reported that their organization has had at least one known case of medical identity theft at their organization. However, only a handful noted that their organizations experienced direct consequences from the breach. And, while most respondents note that their organizations are taking a proactive stance to evaluating and addressing the risk and impact of medical identity theft at their organization, most respondents are not highly concerned that their organization is at risk of medical identity theft in the future.

One-third of respondents (32 percent) reported that their organization has had at least one known case of medical identity theft at their organization. This represents an increase from the 2008 study, when 20 percent of respondents indicated that their organization had at least one known case of medical identity theft at their organization. For the purposes of this research, medical identity theft was identified as "the use of an individual's identity-specific information such as name, date of birth, social security number, insurance information, etc. without the individuals' knowledge or consent to obtain medical services or goods. It may also extend to cases where an individual's beneficiary information is used to submit false claims in such a manner that an individual's medical record or insurance standing is corrupted, potentially impacting patient care".

Among those respondents who had experienced a security breach, only a handful (11 percent) reported that their organization experienced any consequences form a case of medical identity theft. These consequences included additional fines, citations, loss of revenue, legal action and being subjected to additional audits from organizations like The Joint Commission.

Respondents were also asked to identify the threat of medical identity theft at their organization. On a scale of one to seven where one is the low value and seven is the high value, respondents have an average score of 4.05, up from 3.66 in the 2008 survey. This suggests that respondents are not overly concerned about the threat of medical identity theft. Indeed, only 18 percent of respondents indicated that their organization's threat of medical identity theft is either a six or a seven.

However, respondents are being proactive about evaluating and addressing the risk and impact of medical identity theft at their organization. Nearly 80 percent of respondents reported that this type of evaluation is part of their overall privacy and security profile and policy. This is up from the 67 percent of respondents that indicated this to be the case in the 2008 survey.

Finally, respondents were asked to identify whether or not they have changed any of their business practices in the past two years relating to the threat of medical identity theft. Respondents were most likely to indicate that they have improved their patient authentification methods, such as requiring picture identification at intake; this was selected by 60 percent of respondents. More than half of respondents (54 percent) also indicated that their organization now has a plan in place to report suspected medical identity theft or other fraudulent activities to appropriate law enforcement and/or regulatory agencies. A full list of changes in business practices are noted below:

- Providing patients with clear notice of the consequences of sharing health coverage data for the purposes of committing health care fraud – 30 percent;
- Monitors or audits care records so as to confirm that services are delivered only to the appropriate recipient – 30 percent;
- Provides patients with simplified Explanation of Benefits (EOB) – 22 percent;
- Providing patients with resources to identify and report suspected medical identity theft or fraudulent activities to management – 20 percent;
- Aides patients in correcting records that have been corrupted by medical identity theft – 16 percent;
- Contacts patients that have sudden extreme changes in healthcare service utilization to verify that care has actually been received – eight percent.

10. Conclusion

Results from the 2009 HIMSS Security Survey suggests that, despite changes to the security and privacy landscape including new legal and regulatory requirements and increasing risk, healthcare organizations have made relatively little change since the assessment of the market that HIMSS conducted in 2008 relating to a number of important areas of the security environment. This is reflected in the responding healthcare organizations' assessment of their own readiness for today's risks and security challenges. Respondents characterized their own maturity level as mid-range, budgets dedicated to security remain low, and many organizations still do not have a formally designated CSO/CISO. Also, organizations often do not have a plan for responding to threats or incidents relating to a security breach.

This year's survey data showed that respondents characterized the maturity of their organization's security program as mid-level (4.27 on a scale of one to seven where one is low and seven is high). Spending on security represents only a small percentage of the overall IT budget and fewer than half of respondents indicated that their organization has a formally designated Chief Information Security Officer or Chief Security Officer.

Nearly half of the respondents do not currently have a plan for responding to threats or incidents relating to a security breach.

Furthermore, risk assessments are not universal among the responding organizations – only three-quarters perform such an assessment. These results are somewhat concerning considering that the operating environment is becoming more complex due to an increase in adoption of health IT, the prospect of increasing levels of data exchange, new laws and regulations, and an increasingly complex threat environment. These factors may put health data at a higher risk of exposure in the future, and increase the need for mature security processes and controls, based on ongoing risk analysis.

Importantly, of those organizations that do actively perform risk assessments, half (52 percent) indicated that patient data at their organization was found to be at risk as a result of both a lack of effective security controls and a lack of adequate policies and/or procedures. Another 15 percent indicated that their organization's patient data was at risk as a result of a lack of effective security controls in place at their organization and five percent indicated that their organization's patient data was at risk because their organization did not have adequate policies and procedures in place. The risk assessment activity positions organizations to correct deficiencies and the survey data serves to emphasize the important role and value that ongoing security risk analysis can play in protecting health data.

The survey also assessed some aspects of healthcare organizations' readiness to comply with the new privacy statutes in American Recovery and Reinvestment Act of 2009 (ARRA) and related upcoming regulation from Health and Human Services (HHS). For example, under ARRA, healthcare organizations are required to provide notification of data breaches to the patient (as well as HHS and the public in some circumstances) and provide accounting of all disclosures of protected health information upon patient request (for the three years prior to the request). This survey specifically addresses some of the tools that organization's use to gather the data necessary to provide this information.

Results showed that audit logs are widely used among the healthcare organizations represented in this survey. Data from firewalls, application logs and server logs are common sources of information retained in the audit logs. However, at this time, only one-quarter of respondents reported that analysis of log data is done entirely electronically. Many respondents reported that they analyze most, if not all, of the information in these logs through manual means (survey data shows that 38 percent of the organizations conduct only manual log review and an additional 36 percent use some combination of automation and manual review). More clinical data is being created/stored/exchanged in electronic form, the volume of data in logs and audit trails continues to grow. Thus, the need to correlate data from various log sources increases, the need for near real-time, automated reviews based on business rules will only become greater. Without the assistance of some automated/electronic means to analyze log data, organizations may not be well positioned to provide patients with a breach notification. In addition, they may have difficulty producing a clear and accurate accounting of disclosures.

In addition, many organizations are not using available technologies to secure data, such as encryption - which is used by just 67 percent of responding organizations - to secure data in transmission and fewer than half encrypt stored data. The use of encryption represents a common security tool to protect data and, with respect to ARRA, can provide a safe harbor for healthcare organizations with respect to breach notification. (That is, if organizations use appropriate means to secure data, they may be exempt from the breach notification requirement for breaches of that data.) Another notable security control area with a low adoption rate is data loss prevention (which helps protect data confidentiality), which is implemented in only one quarter of the responding organizations.

Nearly all respondents reported that they currently share data with other organizations and the number of respondents that plan to share information externally in the future is increasing. For instance, the number of respondents participating in a health information exchanges (HIEs) is projected to triple in the future among organizations participating in this survey. This increased data sharing will provide added pressure for organizations to be "good business partners" – that is, to be good stewards of that they store and exchange. Finally, state and federal laws and regulations for data exchange, and HIE enterprise data sharing agreements also will apply.

Healthcare organizations today face increasing challenges as they are being urged to adopt electronic health records in the midst of a complex legal, regulatory and risk environment. To effectively secure patient data, it is important that organizations appropriately resource and manage their security initiatives. Trends as reflected in the survey results indicate that organizations are currently required to be extremely efficient in terms of how they are using their resources. These factors will become even more critical factors in the future, as organizations will have to continue to deal an increasingly complex operating environment.

11. About HIMSS

The Healthcare Information and Management Systems Society (HIMSS) is a comprehensive healthcare-stakeholder membership organization exclusively focused on providing global leadership for the optimal use of information technology (IT) and management systems for the betterment of healthcare. Founded in 1961 with offices in Chicago, Washington D.C., Brussels, Singapore, and other locations across the United States, HIMSS represents more than 23,000 individual members, of which 73% work in patient care delivery settings. HIMSS also includes over 380 corporate members and nearly 30 not-for-profit organizations that share our mission of transforming healthcare through the effective use of information technology and management systems. HIMSS frames and leads healthcare public policy and industry practices through its educational, professional development, and advocacy initiatives designed to promote information and management systems' contributions to ensuring quality patient care.

12. About Symantec

Symantec is a global leader in providing security, storage and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. More information is available at www.symantec.com.

13. How to Cite This Study

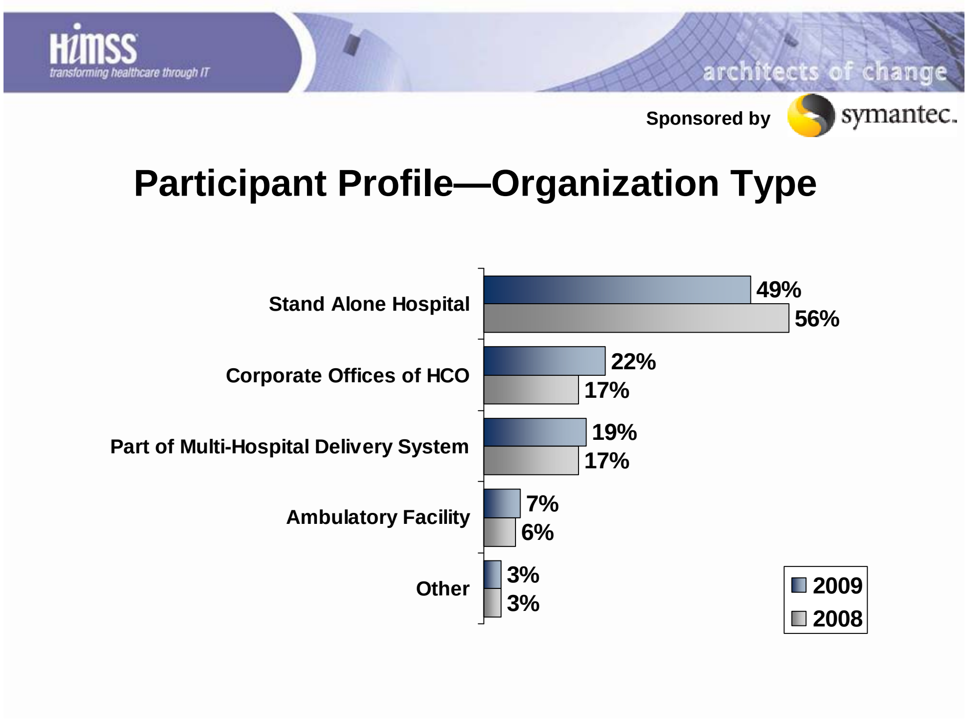
Individuals are encouraged to cite this report and any accompanying graphics in printed matter, publications, or any other medium, as long as the information is attributed to the 2nd Annual HIMSS Security Survey, sponsored by Symantec.

14. For More Information, Contact:

Joyce Lofstrom
Senior Manager, Corporate Communications
HIMSS
230 E. Ohio Street, #500
Chicago, IL 60611
312-915-9237
jlofstrom@himss.org

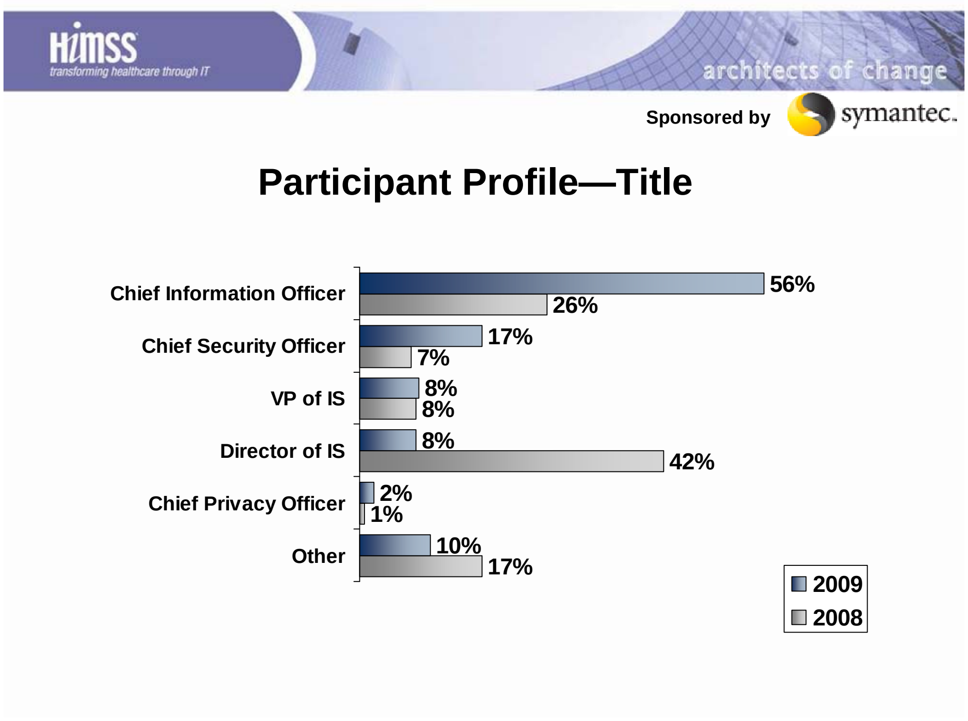
John Lazarus
Senior Manager, Healthcare Industry Solutions
Symantec
275 Second Avenue
Waltham, MA 02451
john_lazarus@symantec.com

Appendix



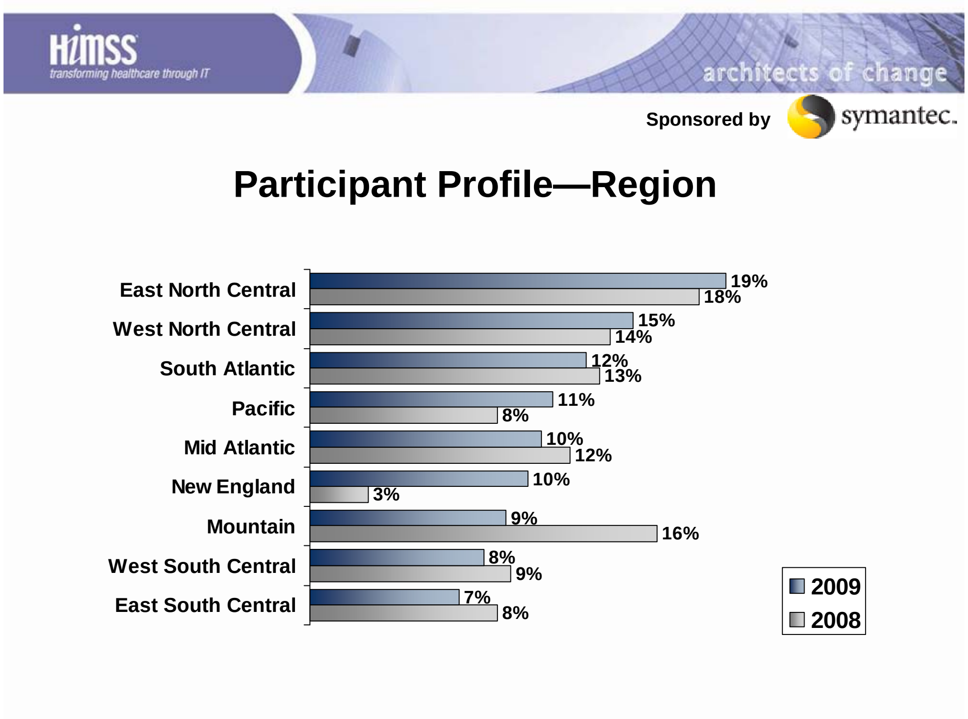
Sponsored by symantec.

Participant Profile—Organization Type



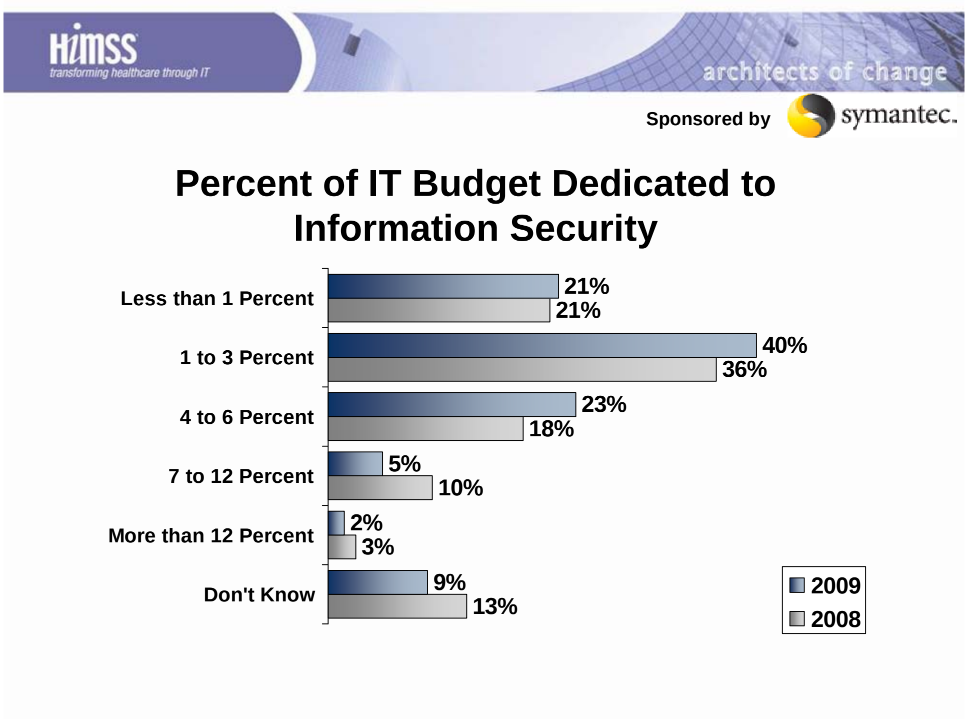
Sponsored by symantec.

Participant Profile—Title



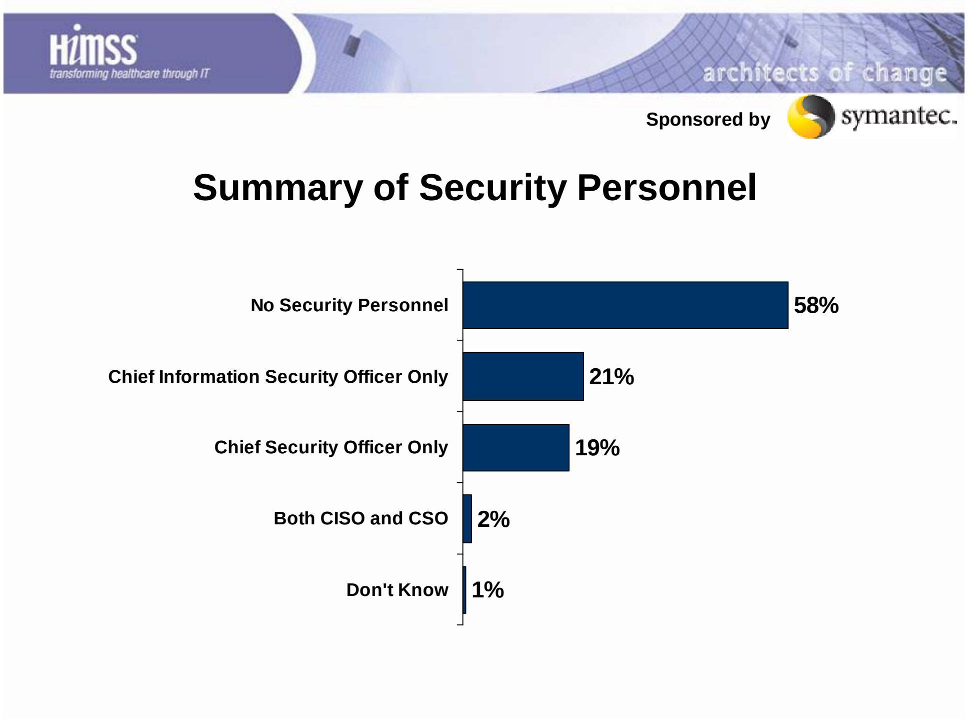
Sponsored by

Participant Profile—Region



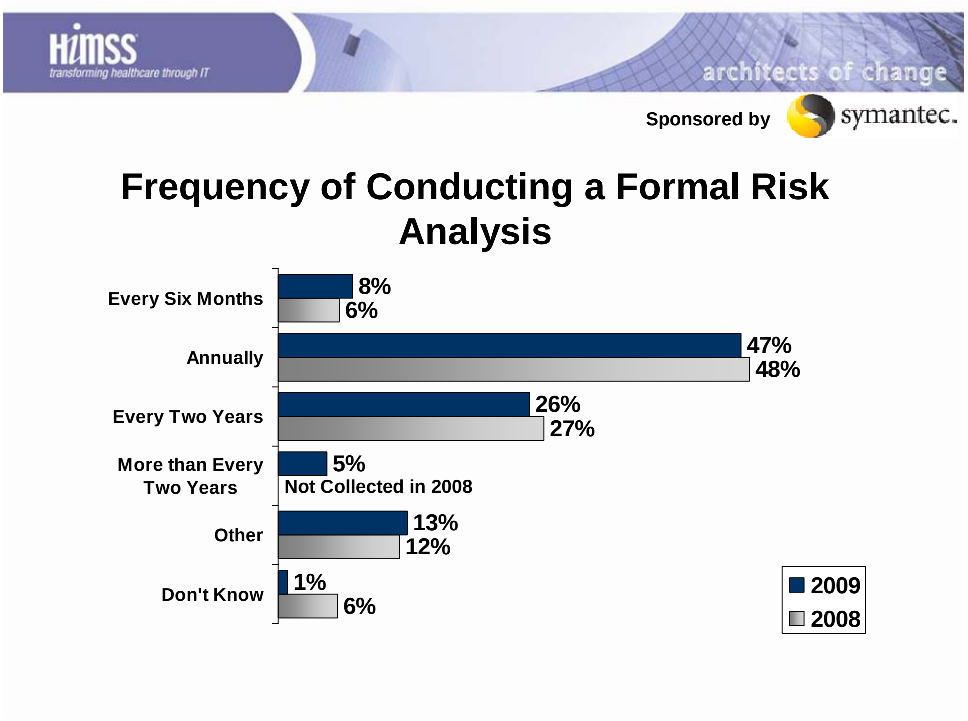
Sponsored by

Percent of IT Budget Dedicated to Information Security



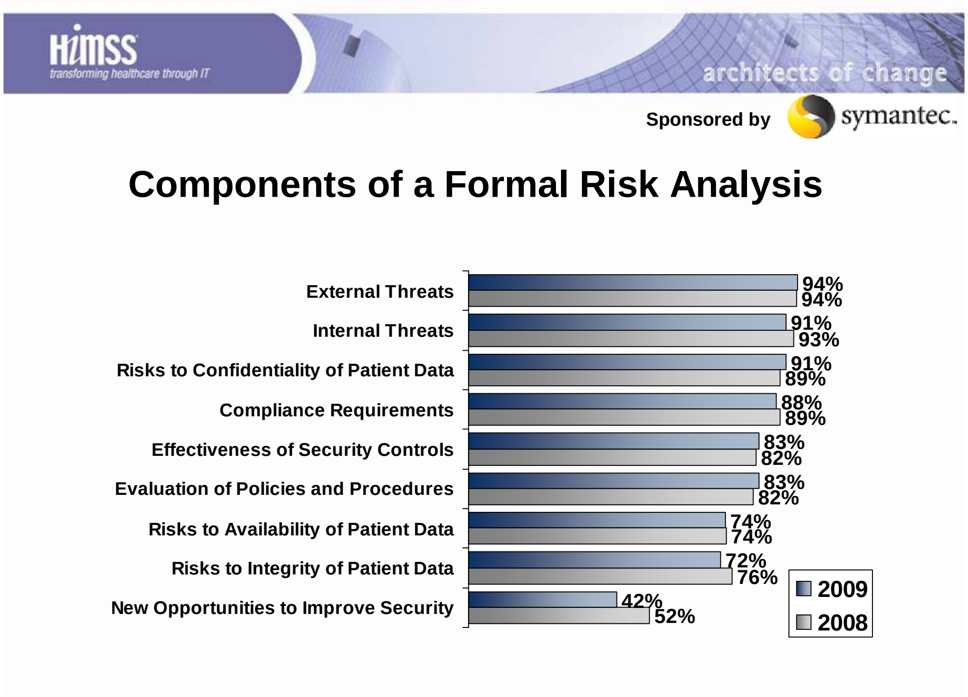
Sponsored by symantec.

Summary of Security Personnel



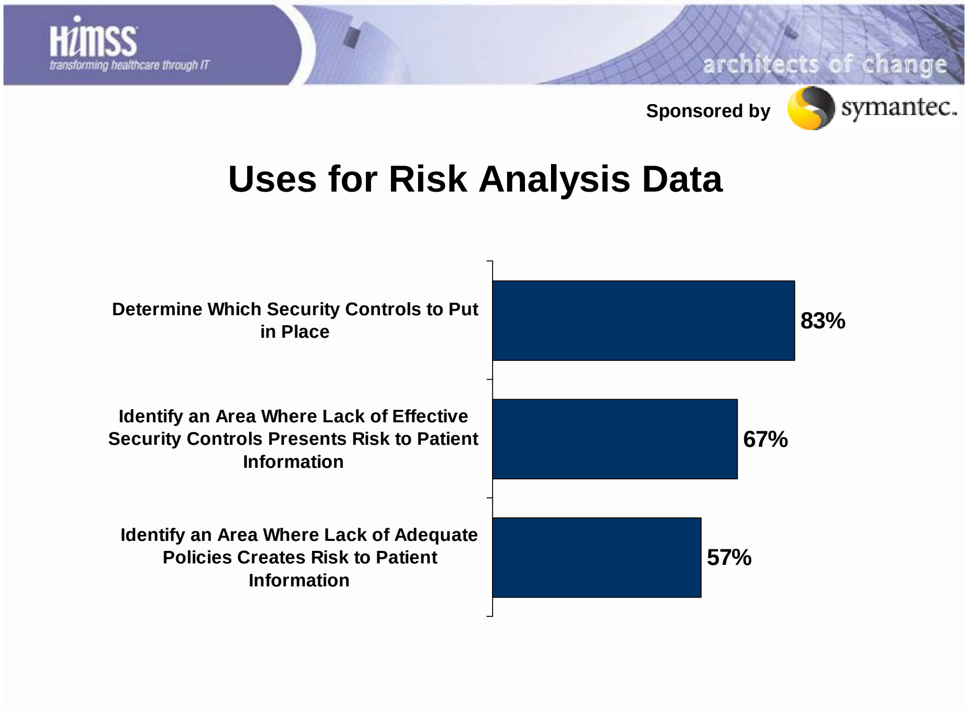
Sponsored by symantec.

Frequency of Conducting a Formal Risk Analysis



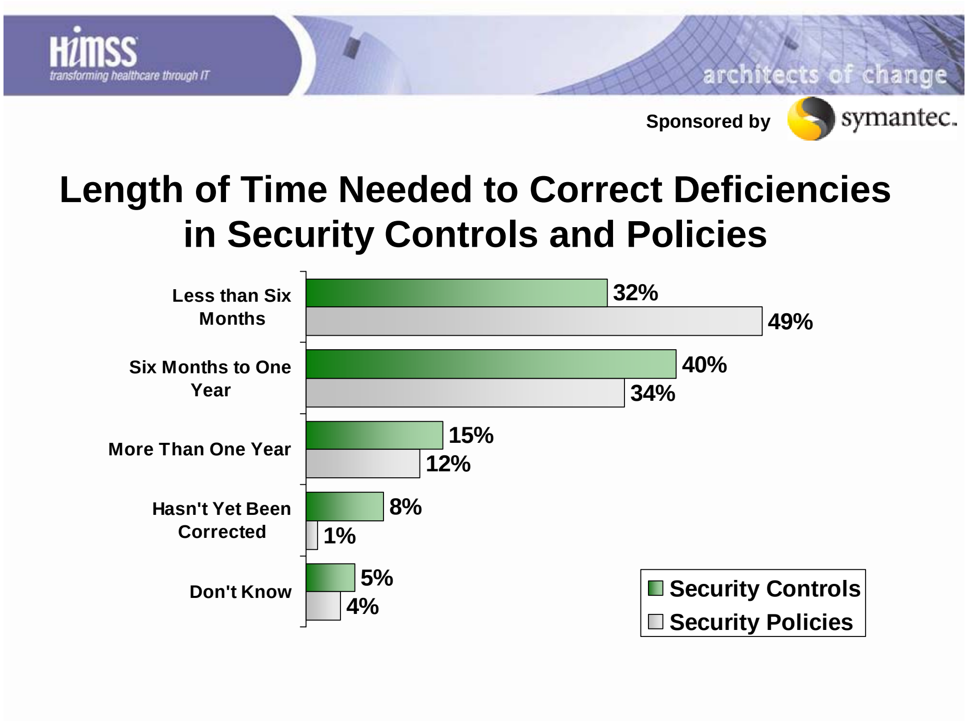
Sponsored by symantec.

Components of a Formal Risk Analysis



Sponsored by symantec.

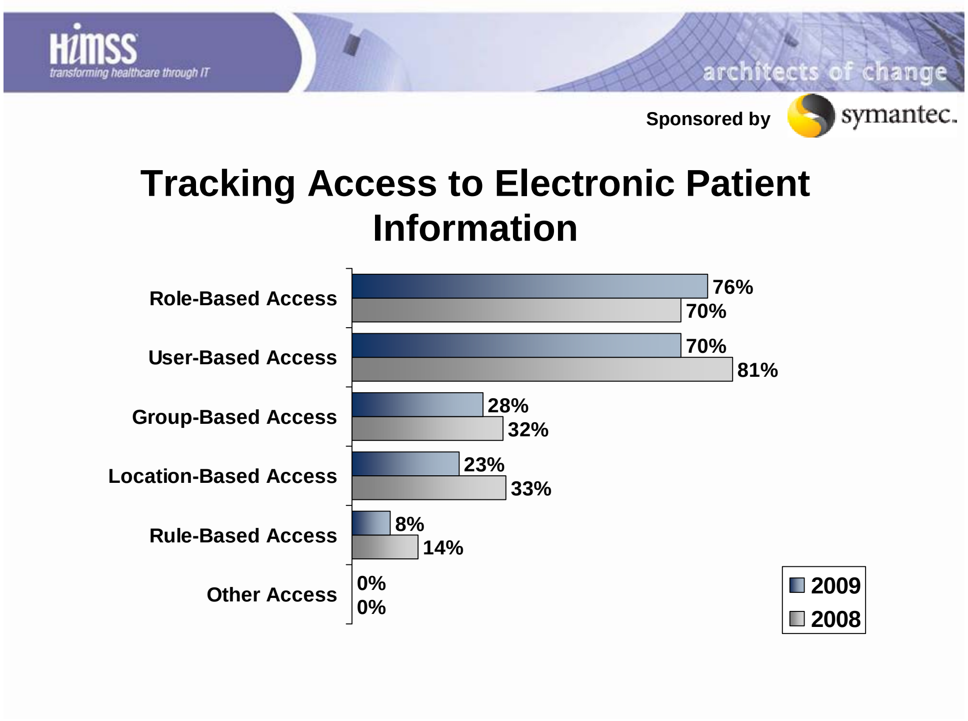
Uses for Risk Analysis Data



HIMSS
transforming healthcare through IT
architects of change

Sponsored by symantec.

Length of Time Needed to Correct Deficiencies in Security Controls and Policies



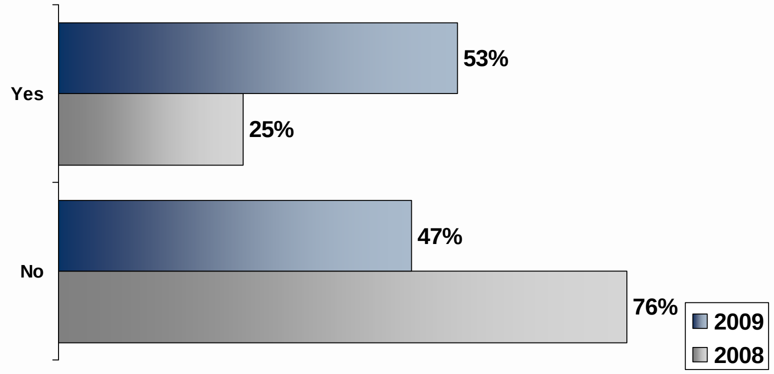
HIMSS
transforming healthcare through IT
architects of change

Sponsored by symantec.

Tracking Access to Electronic Patient Information

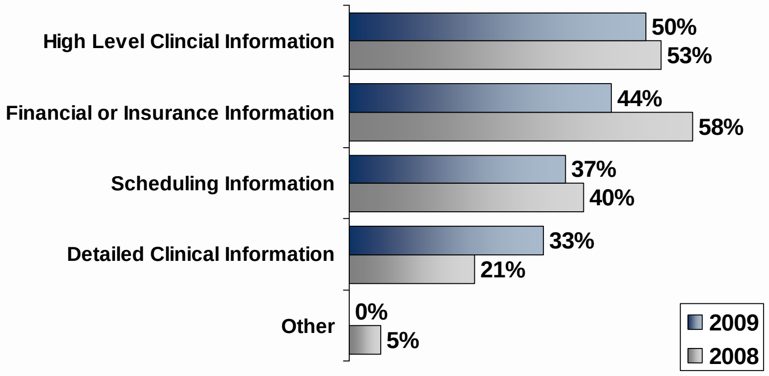
Sponsored by symantec.

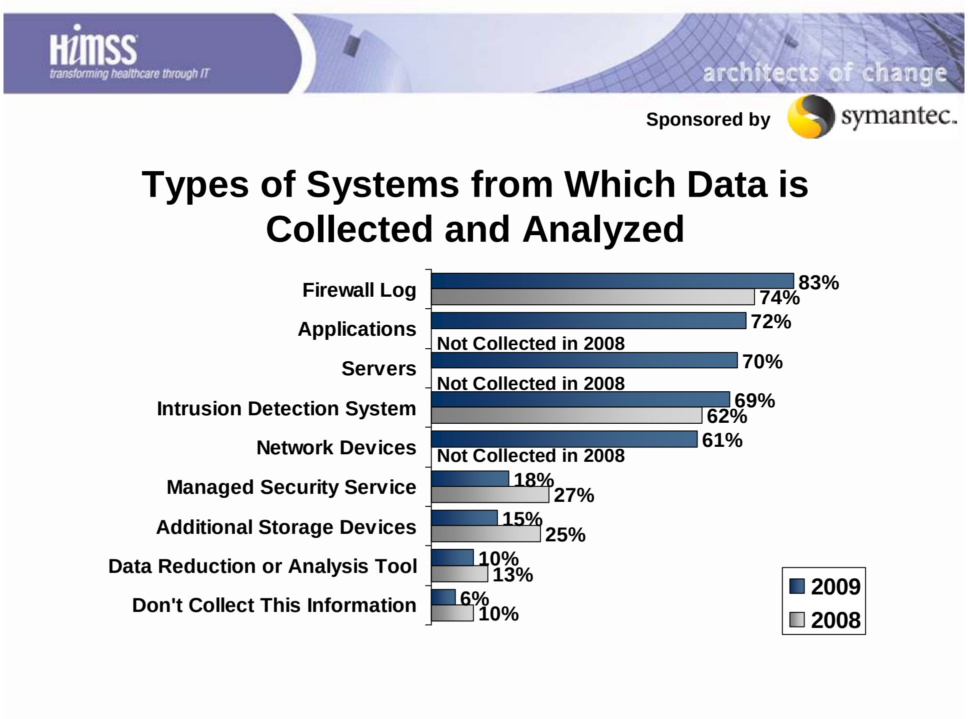
Access of Electronic Data by Patients/Surrogates



Sponsored by symantec.

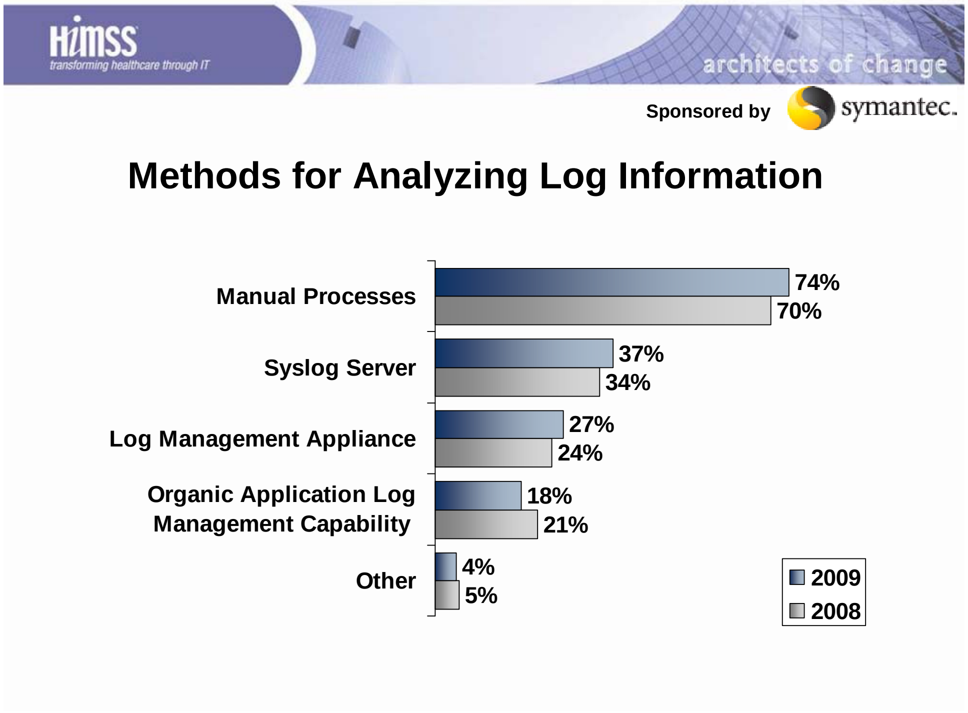
Type of Data Patients/Surrogates can Access





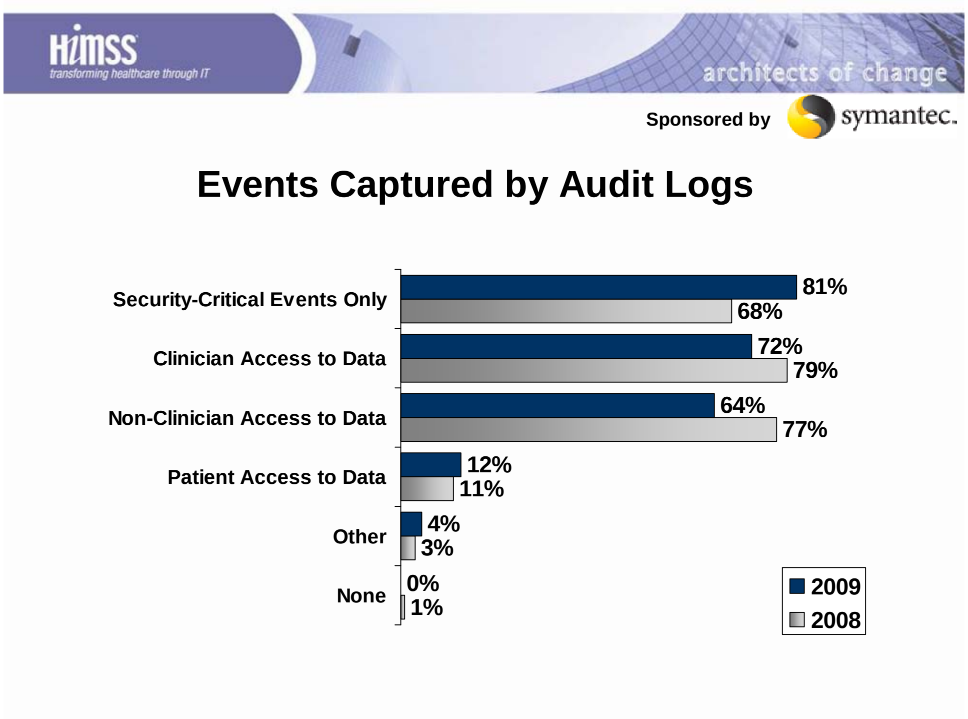
Sponsored by symantec.

Types of Systems from Which Data is Collected and Analyzed



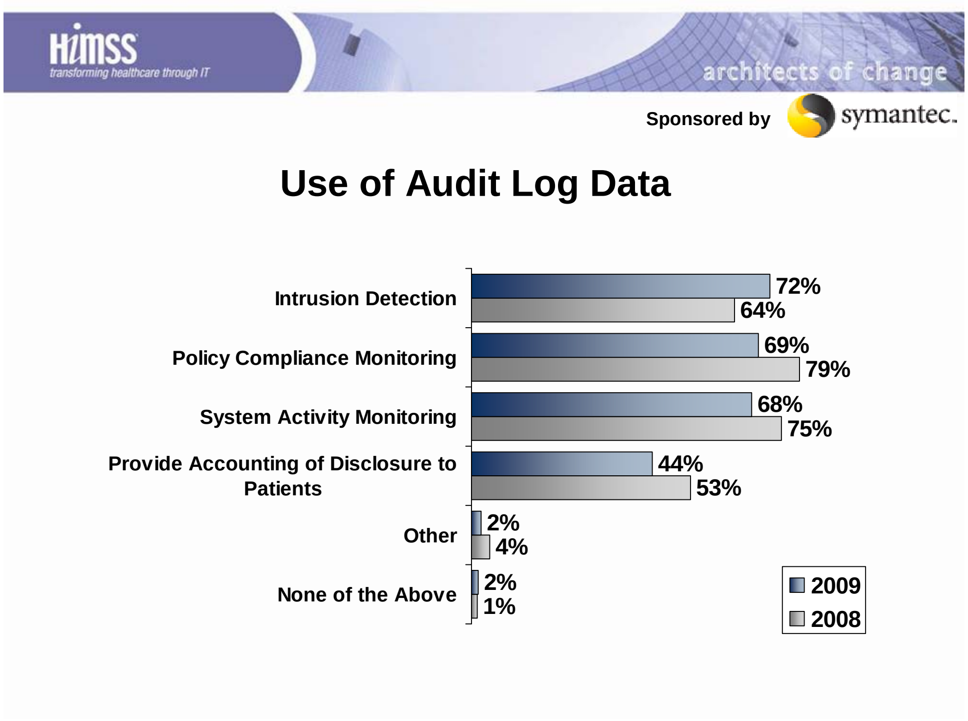
Sponsored by symantec.

Methods for Analyzing Log Information


HIMSS transforming healthcare through IT architects of change

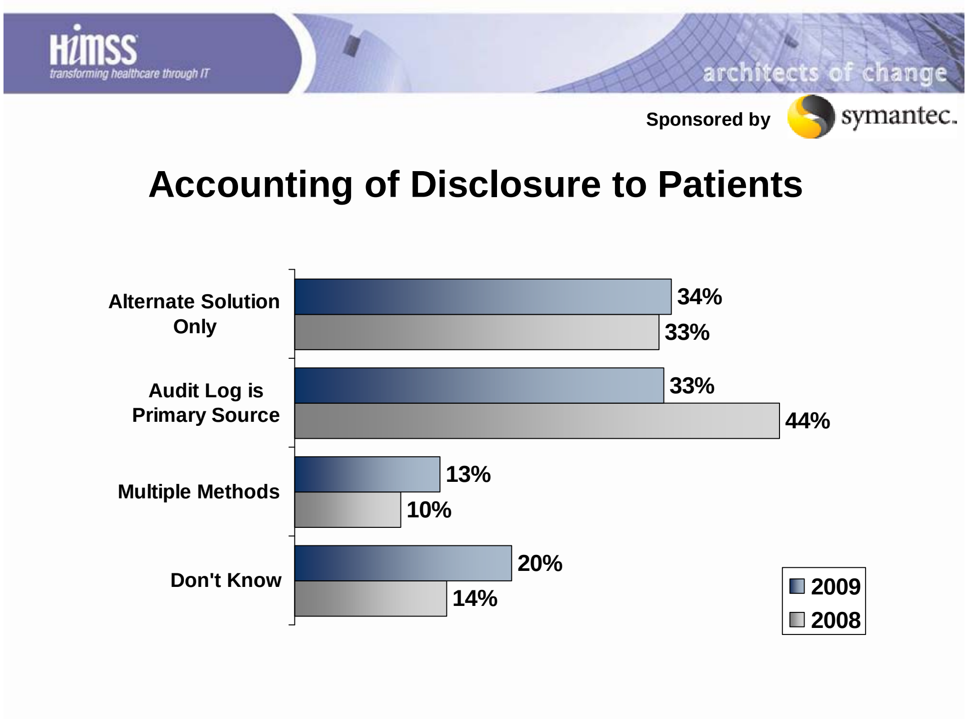
Sponsored by symantec.

Events Captured by Audit Logs

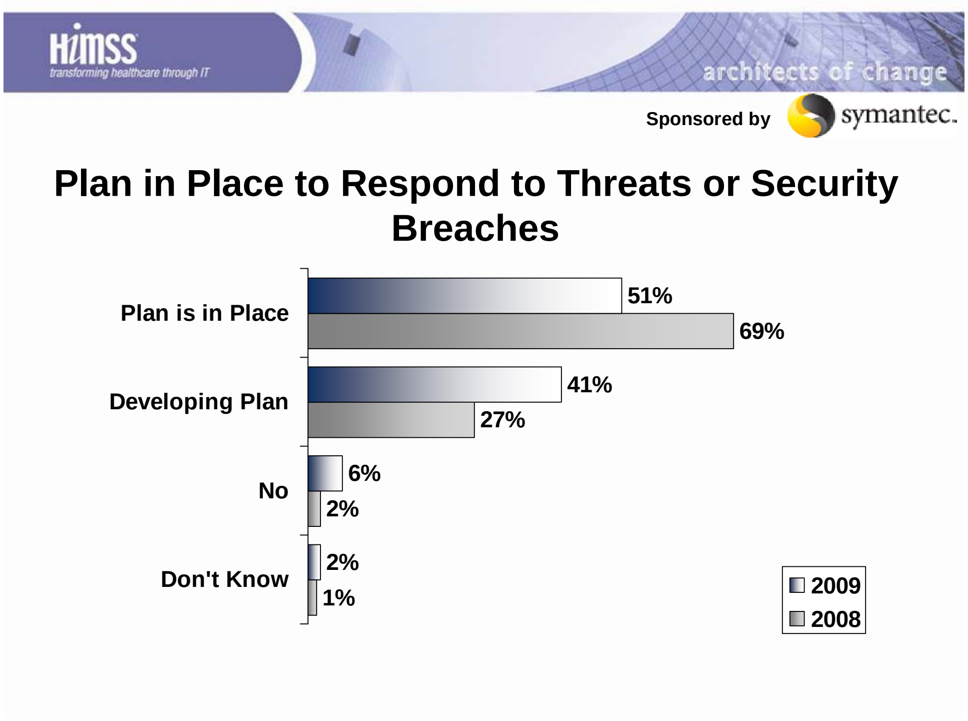

HIMSS transforming healthcare through IT architects of change

Sponsored by symantec.

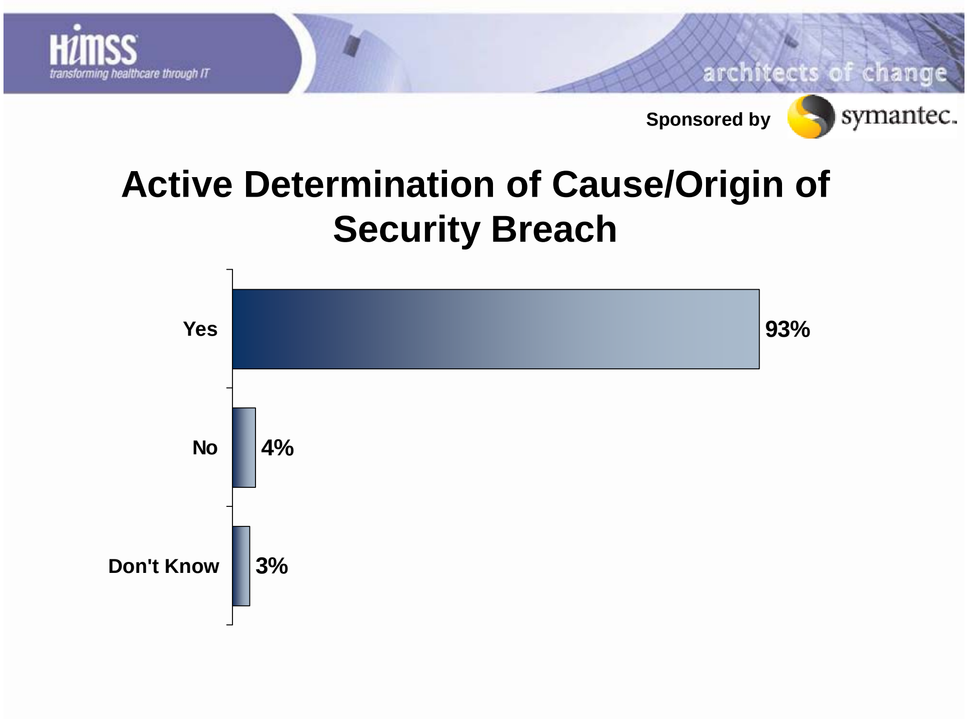
Use of Audit Log Data



Accounting of Disclosure to Patients

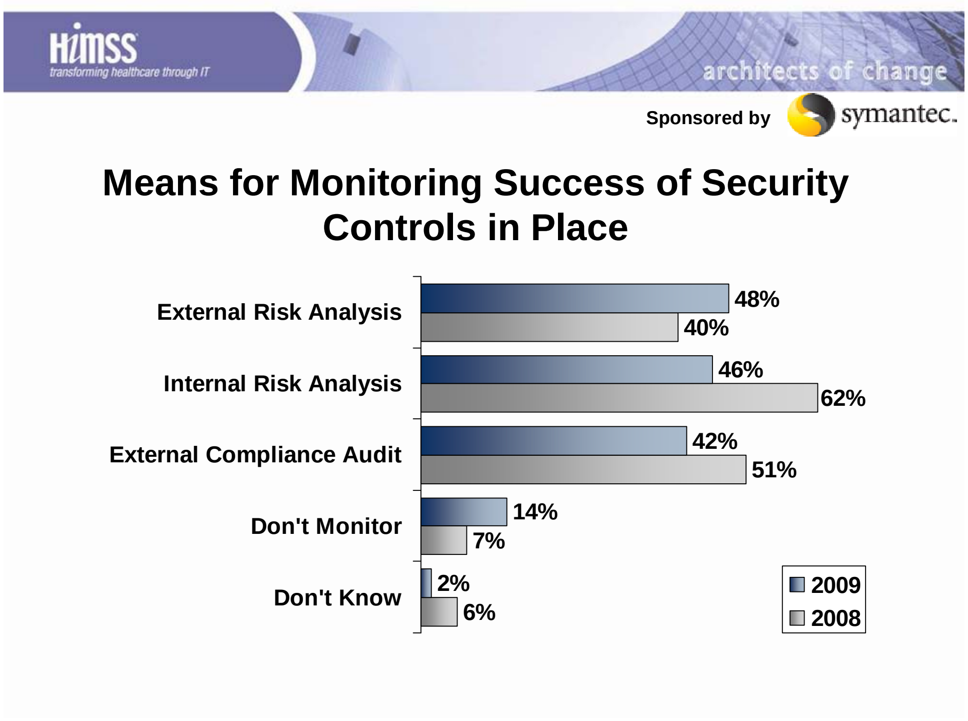


Plan in Place to Respond to Threats or Security Breaches



Sponsored by symantec.

Active Determination of Cause/Origin of Security Breach



Sponsored by symantec.

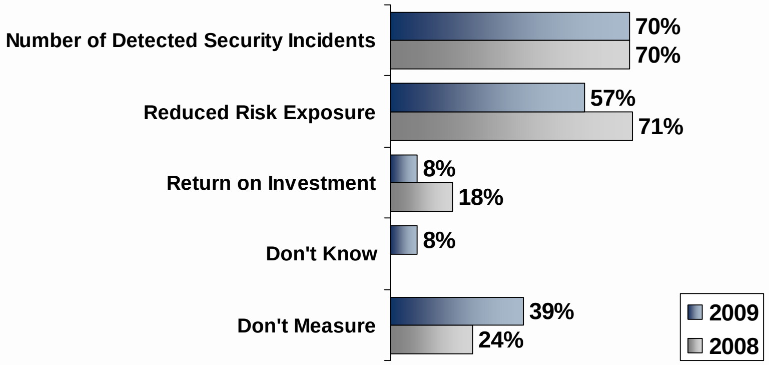
Means for Monitoring Success of Security Controls in Place

HIMSS
transforming healthcare through IT

architects of change

Sponsored by symantec.

Means for Measuring Success of Security Controls in Place

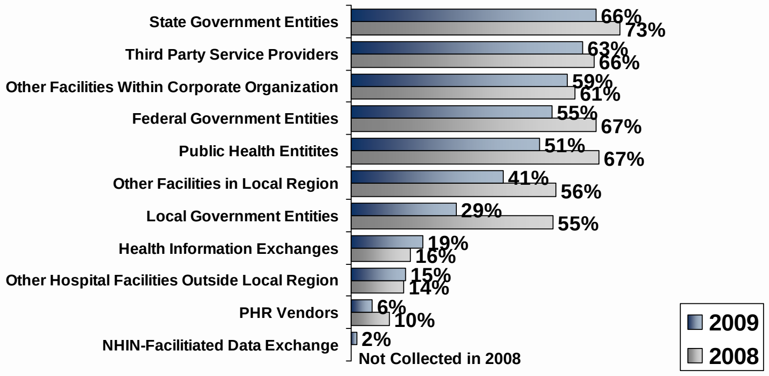


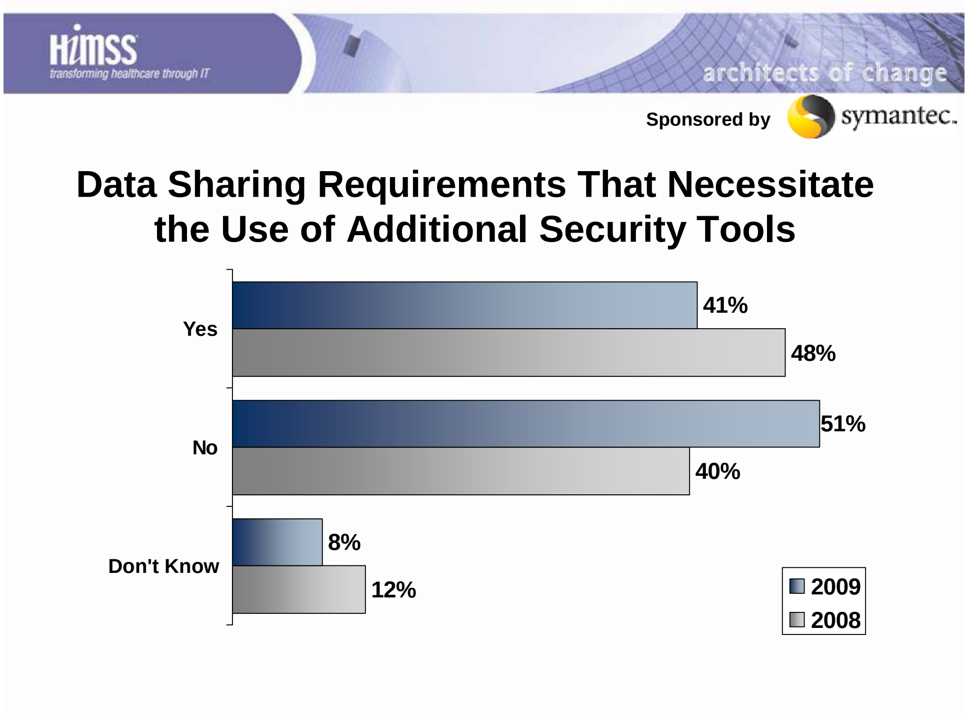
HIMSS
transforming healthcare through IT

architects of change

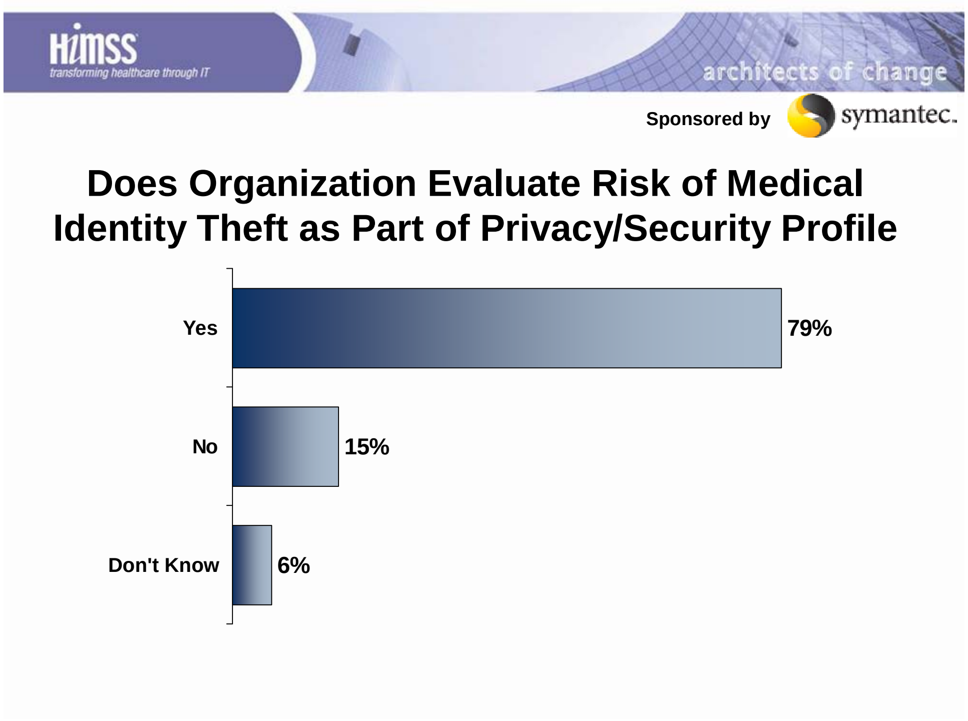
Sponsored by symantec.

Existing Data Sharing Relationships

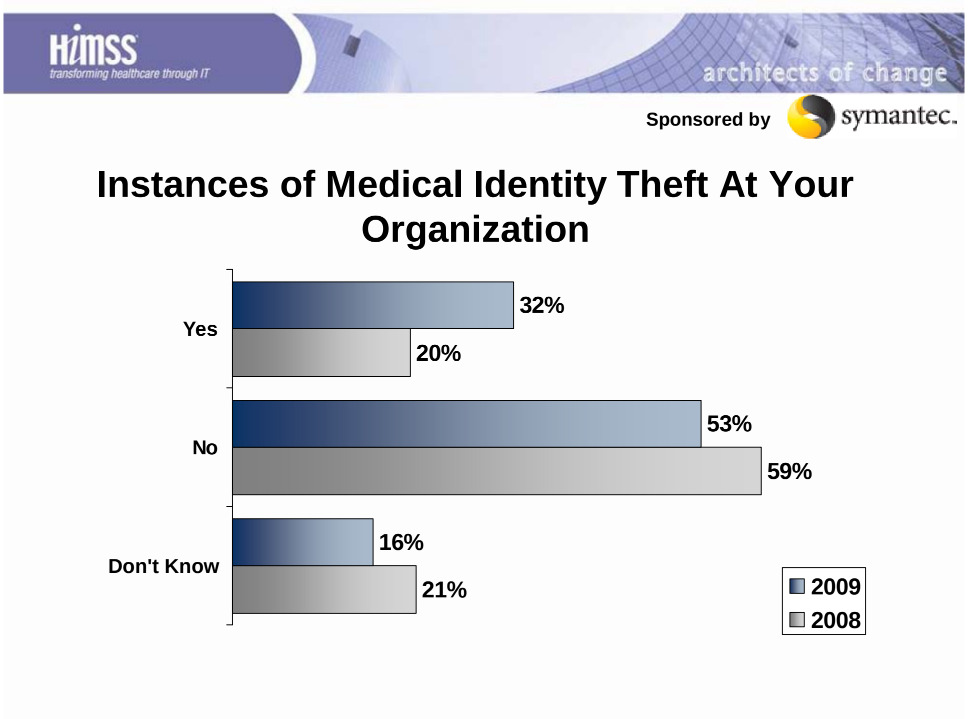




Data Sharing Requirements That Necessitate the Use of Additional Security Tools

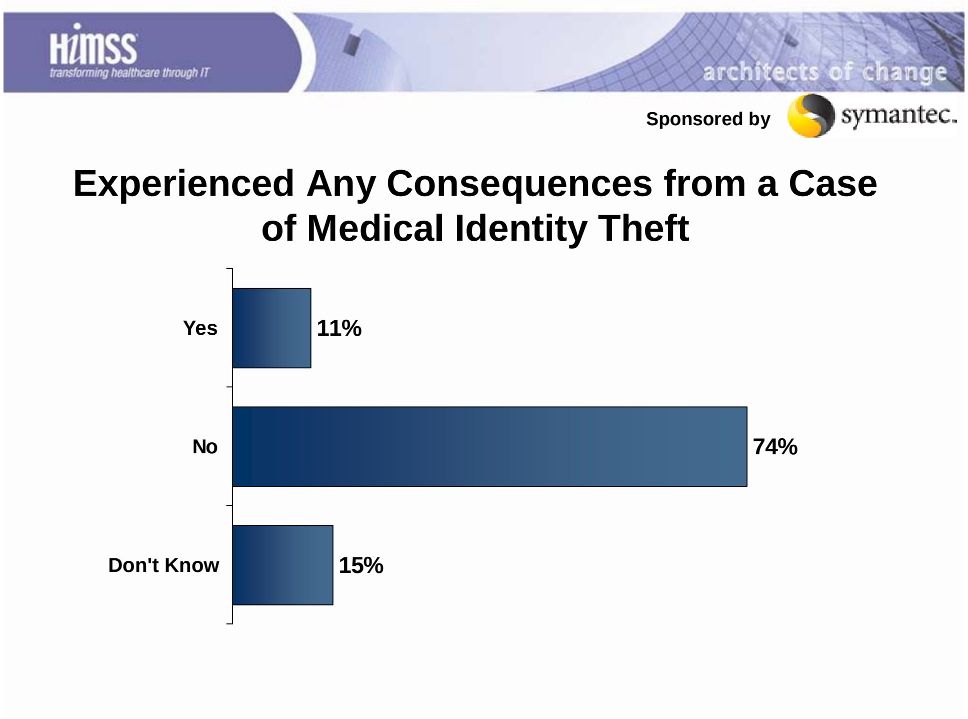


Does Organization Evaluate Risk of Medical Identity Theft as Part of Privacy/Security Profile



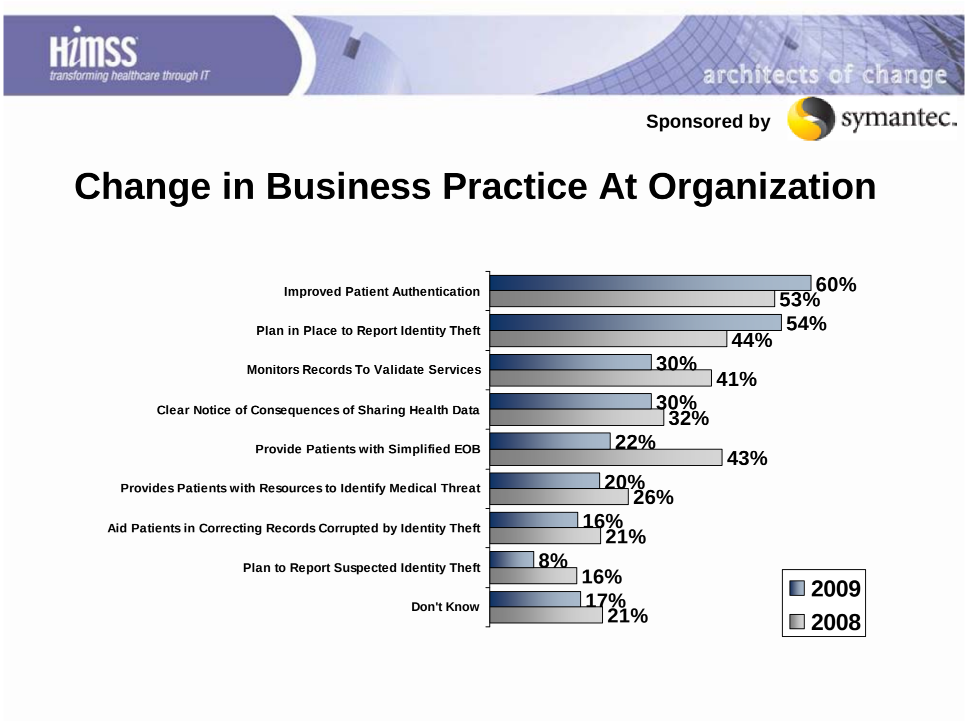
Sponsored by

Instances of Medical Identity Theft At Your Organization



Sponsored by

Experienced Any Consequences from a Case of Medical Identity Theft



HIMSS transforming healthcare through IT

architects of change

Sponsored by symantec.

Change in Business Practice At Organization