



A Need for a Common Security Framework:
**Survey of Attitudes towards
Information Security in the
Health Care Industry**

Prepared by:

KRC RESEARCH

February 2008

I. METHODOLOGY

KRC Research conducted 150 telephone interviews with health care IT security executives in the United States between January 28 and February 15, 2008 on behalf of the Health Care Information Trust Alliance (HITRUST).

The survey included executives representing companies and organizations from across a variety of sectors that compose the health care industry. All are involved in some way in the transfer of sensitive health care data. The number of interviews that were conducted in each of these sectors (a stratified sample) was designed to match the composition which HITRUST is applying to its framework development program¹. The survey included mid-level, senior and C-suite managers from the following vertical segments (and their percentage of the survey responses):

- 63% Health care provider organizations (health systems, hospital, ambulatory, chronic, long term care, etc.);
- 17% Health plans and pharmaceutical benefits managers;
- 14% Pharmaceutical, biotech, medical supply or medical device manufacturers;
- 5% Wholesale distributor, retailer or mail order pharmacies; and,
- 1% Information networks, clearinghouse or data exchanges.

All companies that were not health care providers or information networks had a minimum annual revenue of \$100 million.

The estimated margin of error for the overall survey sample is ± 8.0 percentage points at the 95% confidence interval.

¹ You can review the criteria for this program at:
<http://www.hitrustalliance.org/HITRUSTCommonSecurityFrameworkOverview.pdf>

II. KEY FINDINGS

1. Clear concerns about security of sensitive information

- ✓ Support for the status quo is *soft* and executives are critical of the security of sensitive information among external partners
 - Though more than eight in ten executives (85%) are satisfied with the overall security of sensitive information in the health care industry, two in three are only *somewhat satisfied*. From another perspective, more than eight in ten executives (82%) are not *very satisfied*
 - Executives with moderate opinions (*somewhat satisfied* and *somewhat confident*) are significantly more critical than those who have strong opinions (such as very satisfied and very confident)
 - Eight in ten executives (79%) are not *very confident* in the security maintained by their external partners
 - Three in four (74%) do not completely trust their external partners to maintain security and privacy

2. There is a broad desire for a common security framework

- ✓ Executives feel common standards and a uniform method of verifying these standards are in place are important goals, long overdue and necessary to avert a major security breach
 - More than eight in ten executives (85%) agreed it is time for the industry to “get together and develop a common set of standards, practices and policies”
 - Two in three agreed (67% agreed, 35% *strongly*) there is going to be a major security breach if action is not taken in the security arena
 - Nearly all executives said it is important (98%, with 86% rating it as *very important*) to have standardized guidelines for all organizations in the health care industry dealing with the security of sensitive medical, personal or financial information
 - And, nearly all said it is important (96%, with 73% *very important*) to have a uniform way to verify whether organizations in the health care industry are properly securing their sensitive information

3. Multiple benefits evident from common security

- ✓ Executives agreed that introducing common standards would improve trust (among customers and amongst each other) as well as mitigate potential liability from information breaches
 - A plurality, almost four in ten (37%), said the biggest benefit of a security framework would be minimizing exposure to information theft, followed by increased customer confidence (29%), and increased compliance with government regulations (28%)
 - In addition, common standards would reduce health costs and raise the level of trust (67% agreed), make it easier to get funding from management (77% agreed) and reduce the time, and expense devoted to auditing (76% agreed)

4. A call for leadership

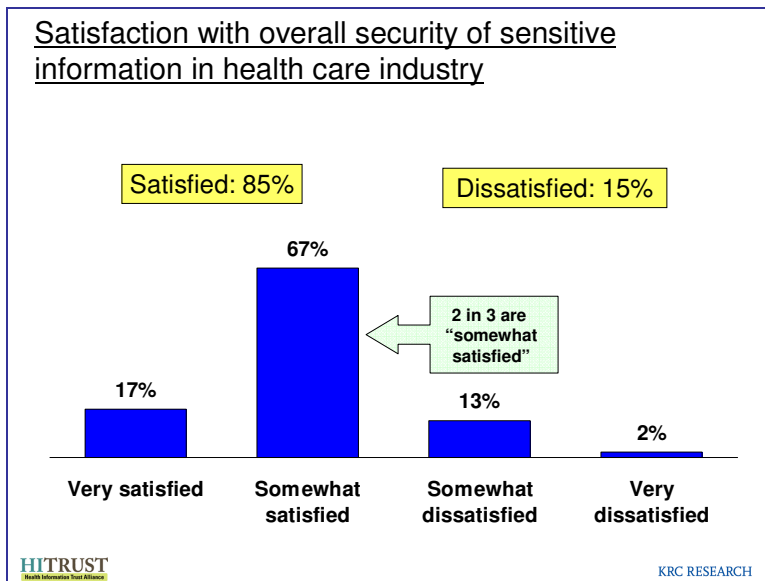
- ✓ Given the interest in common standards and the lack of a technological barrier, a reasonable conclusion is the industry is looking for leadership to organize and develop a set of standards
 - A strong majority (85%) agreed the technology is already available to secure sensitive information
 - A majority (55%) agreed they are *frustrated* that standards are not in place for complying with HIPAA
 - The greatest barrier to developing these guidelines is a lack of cooperation among security executives (cited by a plurality, 37%)

III. DETAILED FINDINGS

LACK OF CONFIDENCE IN EXISTING SECURITY

The data indicates that the vast majority of executives have concerns about the state of data security in the health care industry.

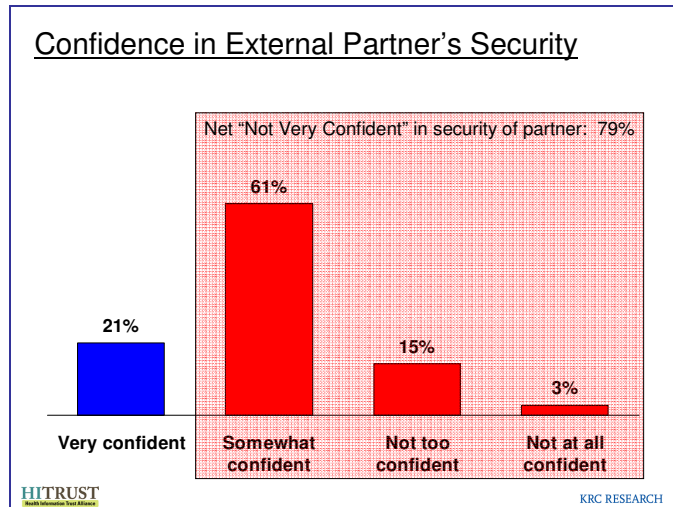
- From the broadest perspective, there is a noticeable lack of support for the industry-wide status quo.
 - At first glance, more than eight in ten executives (85%) indicated they are satisfied with the overall security of sensitive information in the health care industry.
 - However, this satisfaction is very soft, as the vast majority—two in three executives—said they are only *somewhat satisfied*. From another perspective, more than eight in ten executives (82%) are not *very satisfied*.



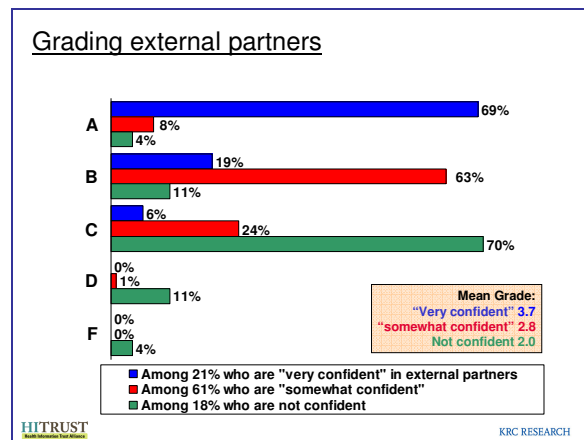
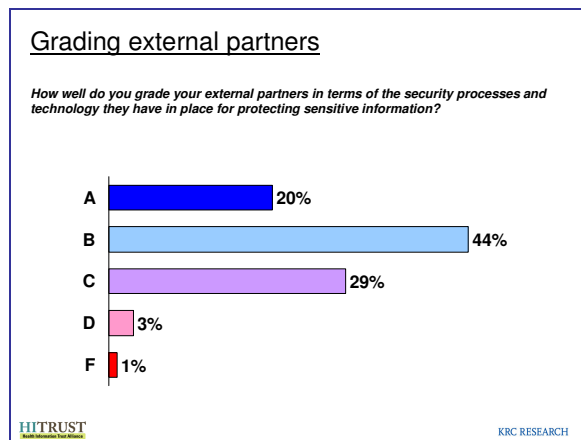
Among security executives in the health industry, in evaluating the state of data security, there are significant differences in attitudes between those who have strong opinions (such as *very satisfied* and *very confident*) and those with moderate opinions (*somewhat satisfied* and *somewhat confident*). By providing context to the strength of opinions, it is clear that only those with strong opinions believe data security is up to snuff and the rest have real concerns and judge the current security among other companies critically.

This point can be illustrated by looking deeper at the attitudinal difference between executives who are *very confident* and *somewhat confident* of external parties.

- Overall, one in five executives is *very confident* in the security of sensitive information at external partners, and six in ten (61%) are *somewhat confident*.



- Executives asked to give a school-letter grade for the security practices of their external partners gave them an average grade of between a B- and a B. Executives who are *very confident* in other companies gave them a grade of an A- and those who are *somewhat confident* rate them an average grade between a B- and a B.

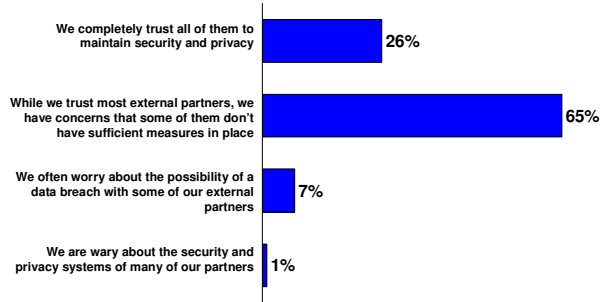


A majority of executives report they do not trust all of their external partners to keep sensitive information secure.

- Another indication that a strong majority of executives are concerned is that three in four (74%) do not completely trust their external partners when it comes to maintaining security and privacy:
 - One in four (26%) said they completely trust external partners to maintain security and privacy;
 - Two in three (65%) trust most partners but have concerns some are not sufficiently secure; and,
 - Less than one in ten (7%) said they often worry about the possibility of a data breach with their external partner.
- As another example of the seriousness of the divide between executives who completely trust their external partners and those who have some concerns, executives graded their external partners' security processes and technology a B+ and B-, respectively.

Level of trust of the information security among external partners

Which of the following best describes how you feel about the information security maintained by your external partners?



HITRUST

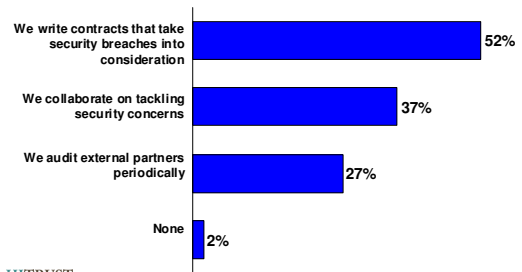
KRC RESEARCH

Most executives surveyed take some sort of proactive steps to build up their trust in the security and privacy measures undertaken by their external partners.

- Half (52%) include penalties in their contracts in the event of security breaches.
- Less than four in ten (37%) collaborate with external partners on dealing with security issues.
- One in four (27%) conduct audits.

Methods for developing trust with external partners

Which of the following, if any, are ways that you develop trust with the security and privacy measures maintained by your external partners? (multiple responses)



HITRUST

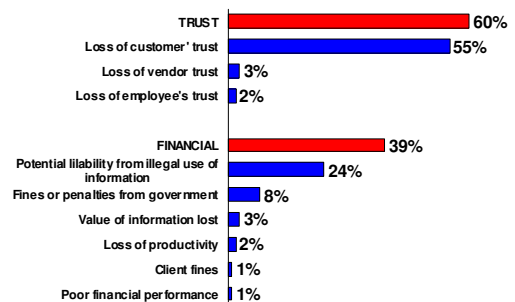
KRC RESEARCH

In the event of a security breach, executives were more likely to be concerned with a loss in reputation than a financial loss.

- A majority (60%) are concerned with a negative impact on their reputation, with most (55%) worried about losing the trust of customers.
- Four in ten (39%) reported their greatest concern is a financial impact, especially from the potential illegal use of the data (24%).

Greatest concerns with security breaches

Which of the following is your greatest concern if your organization mishandled sensitive medical, personal or financial information?



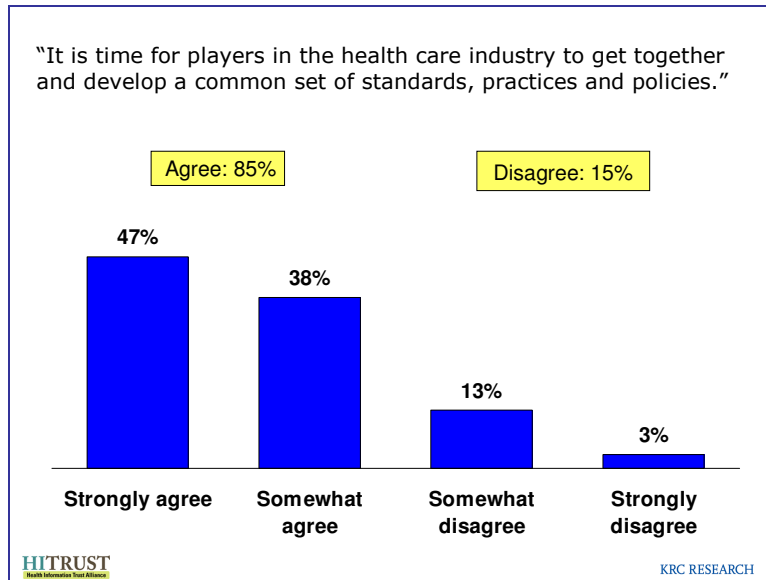
HITRUST

KRC RESEARCH

BROAD DESIRE FOR A COMMON SECURITY FRAMEWORK

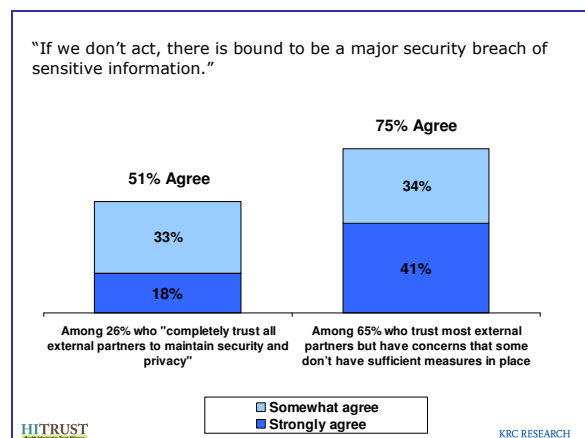
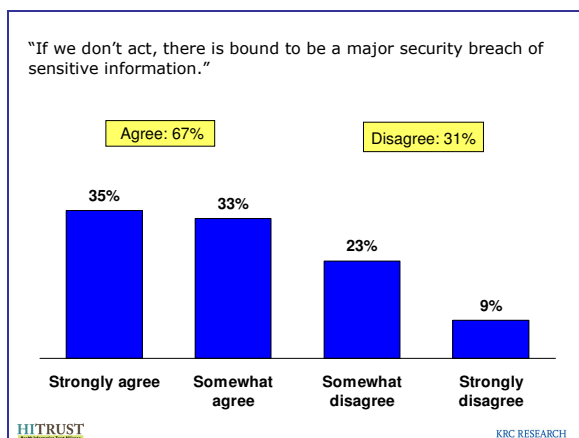
There are several clear indications of a strong desire among executives to clarify how companies are expected to handle sensitive health care information.

- More than eight in ten executives (85%) agreed it is time for the industry to “get together and develop a common set of standards, practices and policies,” including nearly half (47%) strongly agreeing.

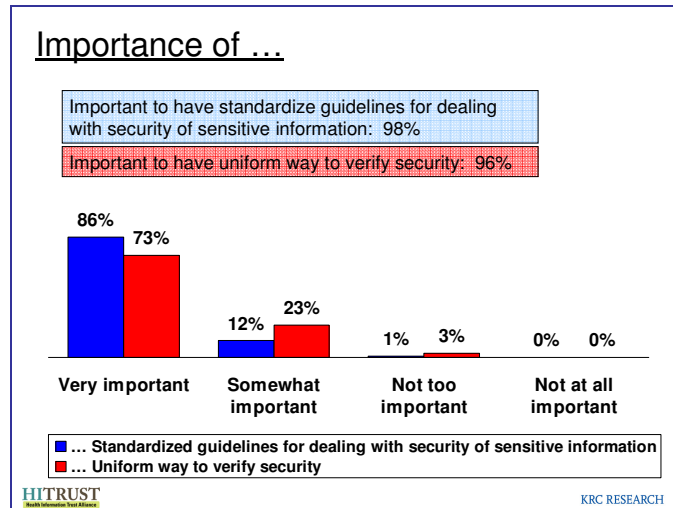


The majority of executives have some concerns about their external partners, and are very concerned about a major security breach by their external partners.

- Two in three executives agreed there is going to be a major security breach if action is not taken on developing common standards, and having them implemented consistently across the industry. More than one in three (35%) felt *strongly* about this.
 - Executives who do not completely trust their external partners (65% who trust most but not all of their external partners) are significantly more likely to have a strong opinion (41% *strongly agree*), especially in comparison to the minority of executives (26%) who trust them (18% *strongly agree*).



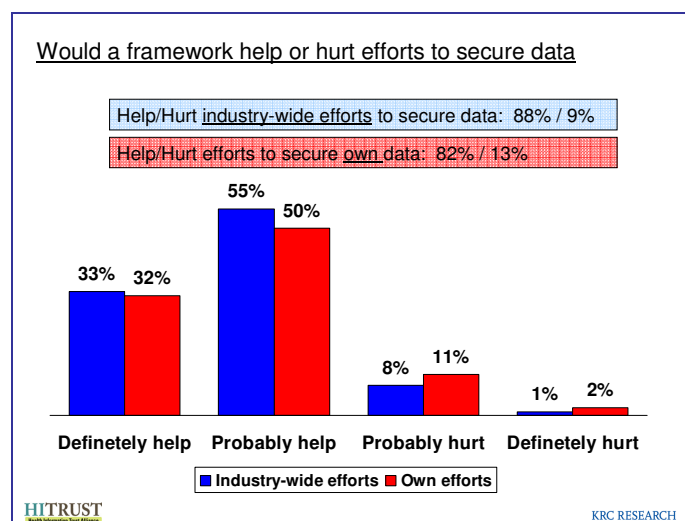
- Nearly all executives (98%) said it is important to have standardized guidelines for all organizations in the health care industry dealing with the security of sensitive medical, personal or financial information, *including 86% who rated this as very important.*
- Likewise, nearly all (96%) said it is important to have a uniform way to verify whether organizations in the health care industry are properly securing their sensitive information, *including 73% who said this is very important.*



EXECUTIVES SEE BENEFITS IN A COMMON SECURITY FRAMEWORK

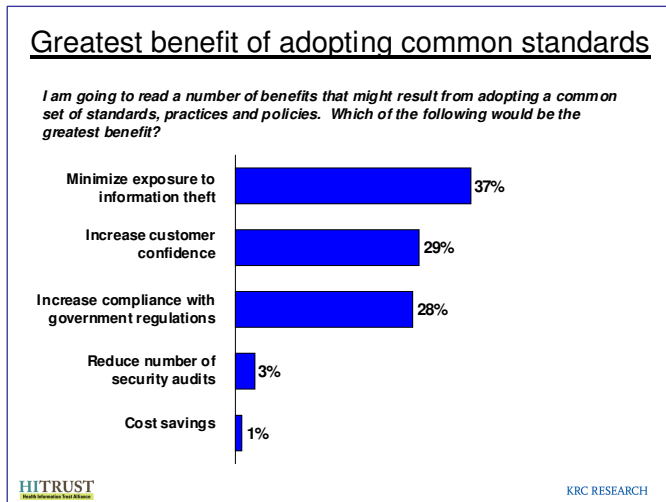
There is broad agreement among executives that a common security framework would help the efforts across the industry and in their own company to secure data.

- Almost nine in ten executives (88%) felt this will help industry-wide. One in three (33%) indicated it would *definitely help*.
- More than eight in ten (82%) thought this would help in their own firm. One in three (32%) felt it would *definitely help*.



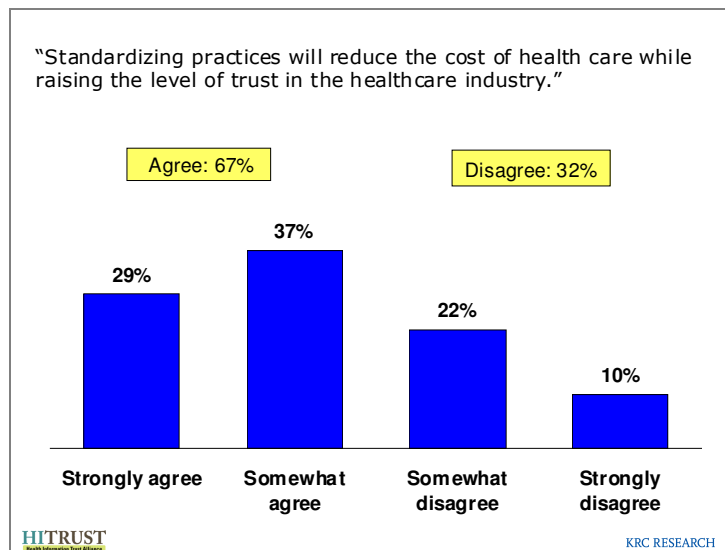
No singular benefit of a common security framework was selected by a majority as the greatest. However, three benefits emerged as popular among executives:

- A plurality of executives, almost four in ten (37%) said the biggest benefit of a security framework would be minimizing exposure to information theft.
- Three in ten (29%) said the greatest benefit would be increasing customer confidence.
- More than one in four (28%) said the greatest benefit would be compliance with government regulations.
- *Increased compliance* was of higher importance among executives who indicated standardized guidelines were very important (32% of them rated this as the top benefit).
Looked at another way, almost all who rated increased compliance as a top benefit (98%) said standardized guidelines were *very important* and 2% rated this as *somewhat important*.

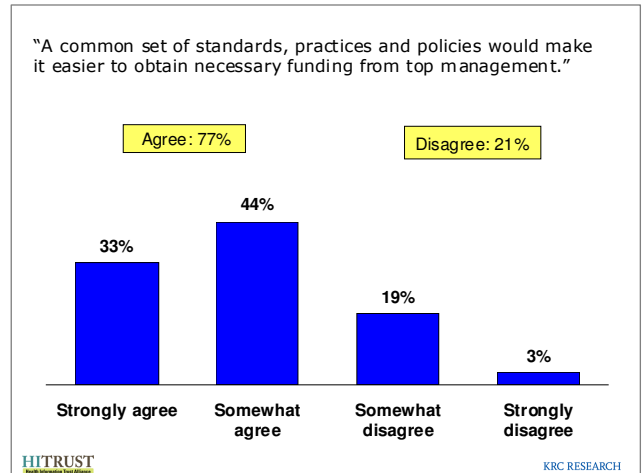


Moreover, there is broad agreement that a common security framework would reduce health costs, raise the level of trust, make it easier to get funding from management, and reduce the time and expense devoted to auditing.

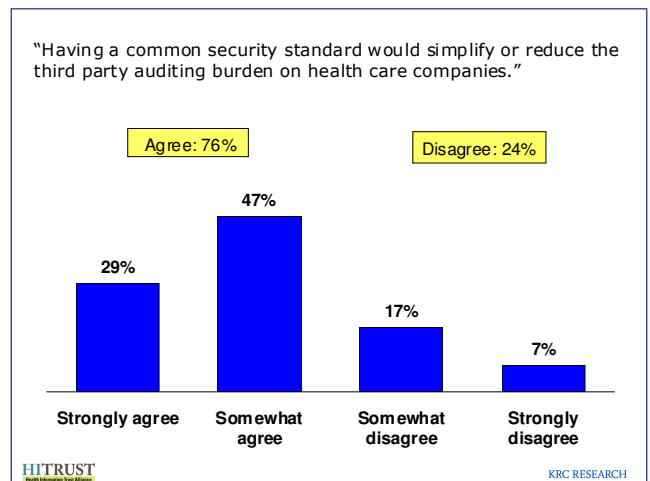
- A strong majority, two in three (67%) agreed that putting a framework into practice would "reduce the cost of health care while raising the level of trust in the health care industry."



- A strong majority of executives, more than three in four (77%), agreed that it would be easier to obtain necessary funding for IT security from their top management if they could point to a set of requirements they had to fulfill.



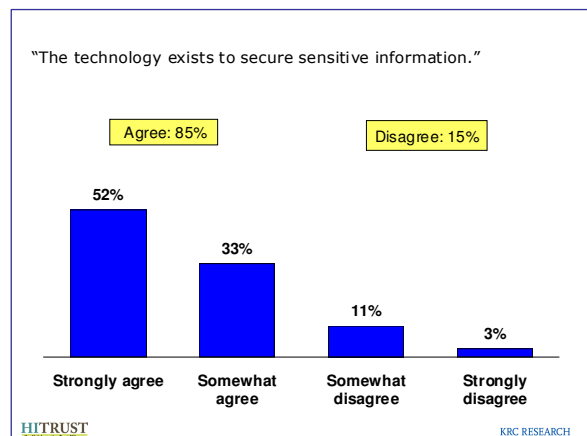
- A strong majority of executives, more than three in four (76%) also agreed that common standards would “reduce the third party auditing burden on health care companies.”



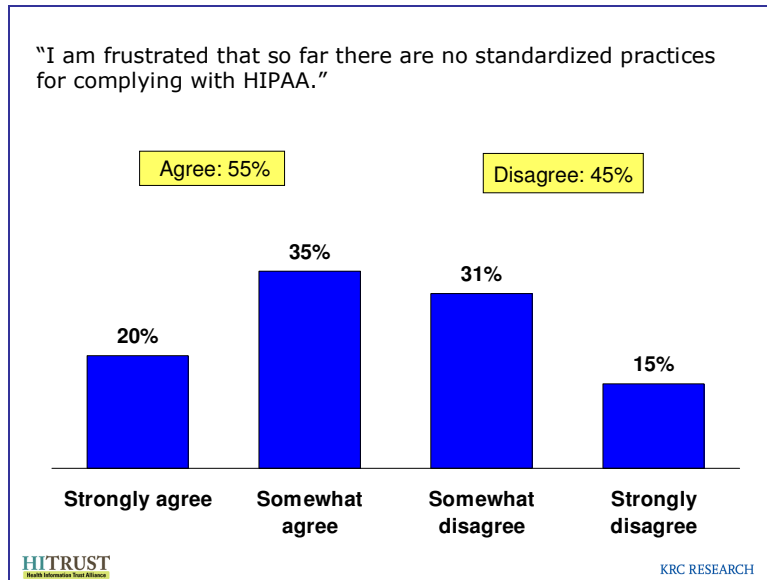
WHERE THERE'S A WILL...

The biggest hurdle to accomplishing a common framework is the willpower in the industry.

- The problem to achieving a common standard is certainly not technical, given that there is strong and broad agreement that “the technology exists to secure sensitive information” (85% agreed, including 52% who strongly agreed).

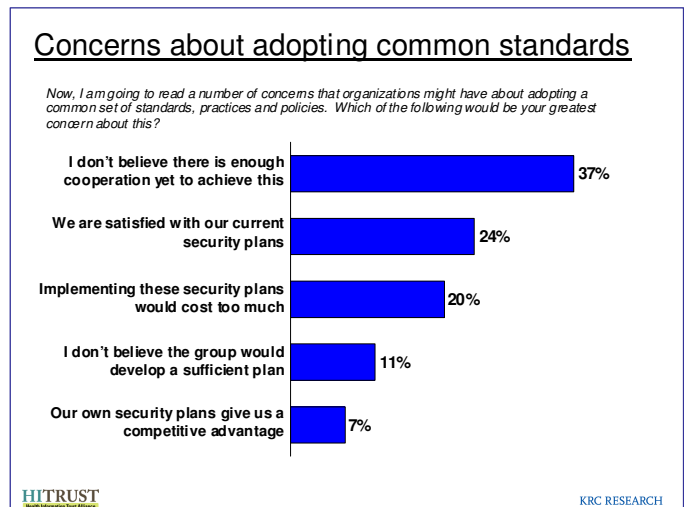


- In addition, a majority of executives already have strong feelings that such a framework should *already* be in place. More than half (55%) indicated they are frustrated that standard practices are not yet in place in the health care industry for satisfying the common HIPAA requirements.



- Asked to select the greatest barrier to developing these guidelines, a plurality of health care security executives (37%) cited a lack of cooperation. In addition:

- One quarter (24%) indicated they were satisfied with their own plans;
- One in five (20%) was concerned the requirements would cost too much;
- One in ten (11%) said they thought the framework would not be sufficient; and,
- Less than one in ten executives (7%) said they were not interested because their own plans gave them an advantage in the marketplace.



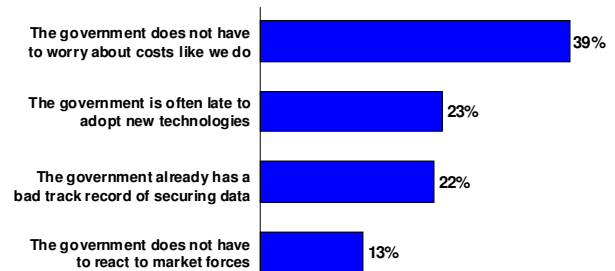
CONCERNS WITH A GOVERNMENT ROLE

Executives expressed a series of concerns with the development of a framework if the government were to assume a leadership role over the process.

- A plurality, four in ten (39%), said they were most concerned the government would be insensitive to the costs that companies in the private industry might have to bear.
- More than one in five (23%) were concerned with the government's record of being late to adopt cutting-edge technology.
- More than one in five (22%) were also concerned with the government's previous history on this topic.
- More than one in ten (13%) indicated their greatest concern was that the government as a public agency does not have to react to market forces.

Greatest concerns about the government taking a leadership role

Suppose the federal government were asked to take a leadership role in the development of a common set of standards, practices and policies for securing sensitive medical, personal and financial information. Which of the following would be your greatest concern about having the federal government play this role?



HITRUST
Health Information Trust Alliance

KRC RESEARCH

##

For more information about the survey or other HITRUST programs, go to www.hitrustalliance.org.