HIPAA Collaborative of Wisconsin

This document is provided "as is" without any express or implied warranty. This document is for educational purposes only and does not constitute legal advice. If you require legal advice, you should consult with an attorney. HIPAA COW has not yet addressed all state preemption issues related to this document. Therefore, this document may need to be modified in order to comply with Wisconsin law.

HIPAA Security Benchmarking Whitepaper

1.0 Introduction

One of the greatest challenges Security Officers and/or Privacy Officers and Compliance Officers face in complying with the HIPAA Security Rule is comprehending what it really means to be "compliant." Because the implementation specifications of the Security Rule are intentionally written to be scalable and flexible, many Covered Entities are uncertain as to whether they are truly compliant with all the standards, and, further, if they were audited by the government, whether or not they would successfully meet the federal requirements as intended in the law.

In the spring of 2009, the HIPAA Collaborative of Wisconsin (COW) Security Networking Group conducted a Benchmarking Survey of Covered Entities across the State of Wisconsin to help define and gauge how and to what level of detail the Security Rule was being implemented. The goal of the Benchmarking Survey was to provide Wisconsin health care organizations with a point of reference on which to focus their compliance efforts. The Security Networking Group was interested in providing a summary of how organizations have interpreted and implemented the regulations to prepare for an audit, thereby providing a type of benchmark against which to gauge an organization's level of compliance.

2.0 Benchmarking Survey Method and Limitations

2.1 Survey Method

The Security Networking Group began by considering the entirety of the HIPAA Security standards and brainstorming to identify particular standards or implementation specifications that were thought to be vague. The Networking Group also considered areas in which it was difficult to determine whether the actions taken or technology implemented to comply with the regulation met the intent of the regulation and would pass a federal audit.

As a result, the particular topics which were identified for the survey were:

- Encryption
- Disaster Recovery

- E-mail Retention
- Automatic Log-out/off
- Password Management
- Portable Media
- Auditing
- Remote Access
- Training
- E-Discovery

The Security Networking Group then painstakingly devised the survey questions for each topic to elicit the most specific and meaningful results. Each set of questions on each topic was also followed by an open-ended question allowing respondents to provide narrative comments.

2.2 Survey Population and Limitations

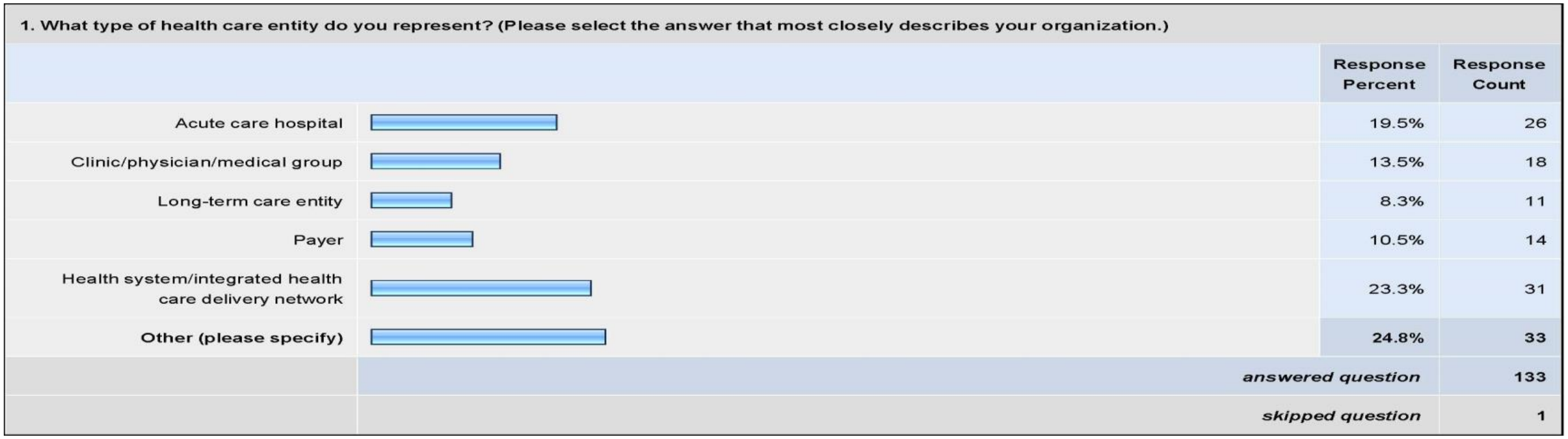
The population surveyed was all those health care organizations in the electronic database of HIPAA COW. The database is comprised of those who have participated in HIPAA COW sponsored conferences since 2001, those who indicated interest in participating in one of the Networking Groups, or anyone who simply wanted to be included in the distribution list of the collaborative. Consequently, the database may contain contact information for more than one individual in a particular organization. The database contains information on approximately 1,500 individuals from health care organizations or vendors who serve the Wisconsin health care industry, although the database is not restricted to Wisconsin – based entities.

To promote the solicitation of responses specific to Covered Entities in the State of Wisconsin and to help ensure that only one response from each Covered Entity was obtained, the introduction to the survey, distributed via e-mail, was addressed to the Security Officer. It was further directed that the survey should be completed by the single individual in the organization who was primarily responsible for HIPAA Security implementation.

Resources available simply did not allow for the further identification of particular individuals to target for receipt of the survey. The intent of conducting this survey was not to generate a statistically valid sample but rather to obtain a fairly representative response to survey questions, the results to simply be used by Wisconsin Covered Entities as a guide for further HIPAA Security implementation. Further, the discussion of the responses to each question summarized below is not meant to be an exhaustive or all-encompassing discussion but simply a guideline from which to work.

2.3 Survey Response

The first set of survey questions identified various types and sizes of health care entities which the Security Networking Group thought were an important consideration in gauging the resources available for Covered Entities to implement the regulations, especially given the costs associated with some of the technology potentially required to comply with the regulations. The results are graphed below.

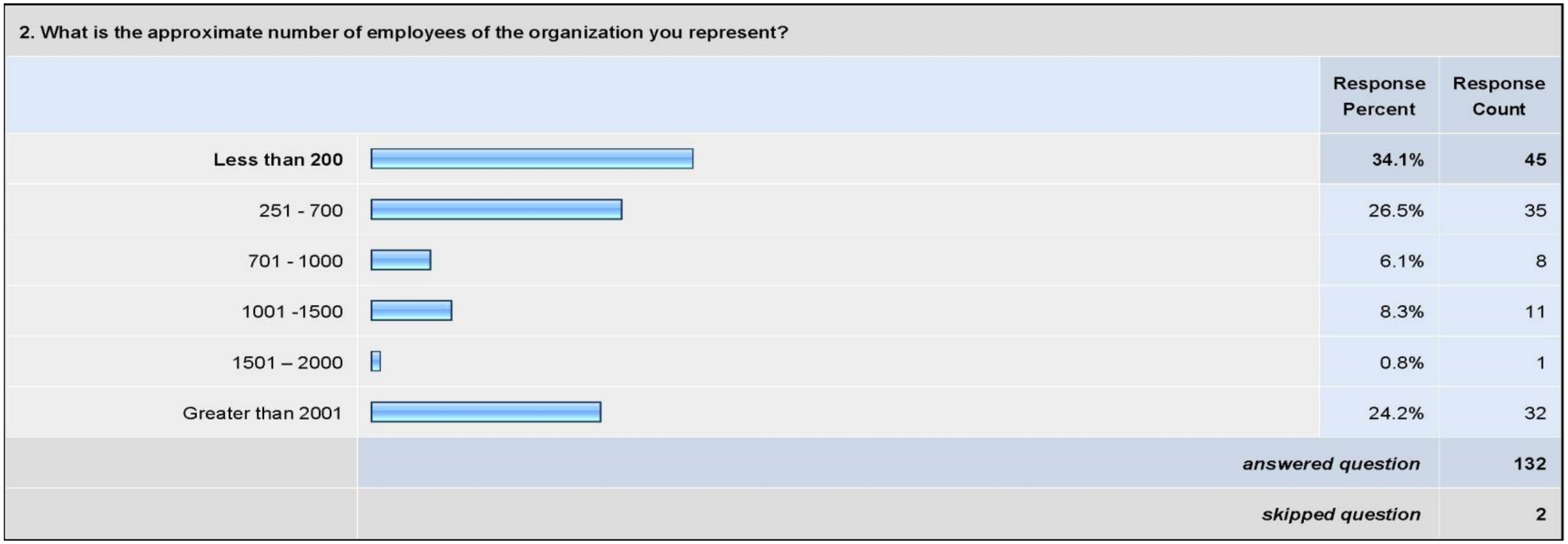


1. What type of health care entity do you represent? (Please select the answer that most closely describes your organization.)

	Response Percent	Response Count
Acute care hospital	19.5%	26
Clinic/physician/medical group	13.5%	18
Long-term care entity	8.3%	11
Payer	10.5%	14
Health system/integrated health care delivery network	23.3%	31
Other (please specify)	**24.8%**	**33**
	answered question	**133**
	skipped question	**1**

Our results, reported as percentages, are based upon a total of 134 respondents. The identity of all participating organizations remained anonymous.

- 23.3% of respondents identified themselves as representing health systems or an integrated health care delivery network
- 19.5% identified themselves as representing an acute care hospital
- 13% of the respondents were from physician or medical groups
- 24.8%, or approximately 1/4, of the respondents were classified as “other”
- The category of “other” was not further defined but potentially captures governmental entities, billing companies, collection agencies, independent labs, rehabilitation facilities, etc.



2. What is the approximate number of employees of the organization you represent?

	Response Percent	Response Count
Less than 200	**34.1%**	**45**
251 - 700	26.5%	35
701 - 1000	6.1%	8
1001 -1500	8.3%	11
1501 – 2000	0.8%	1
Greater than 2001	24.2%	32
	answered question	**132**
	skipped question	**2**

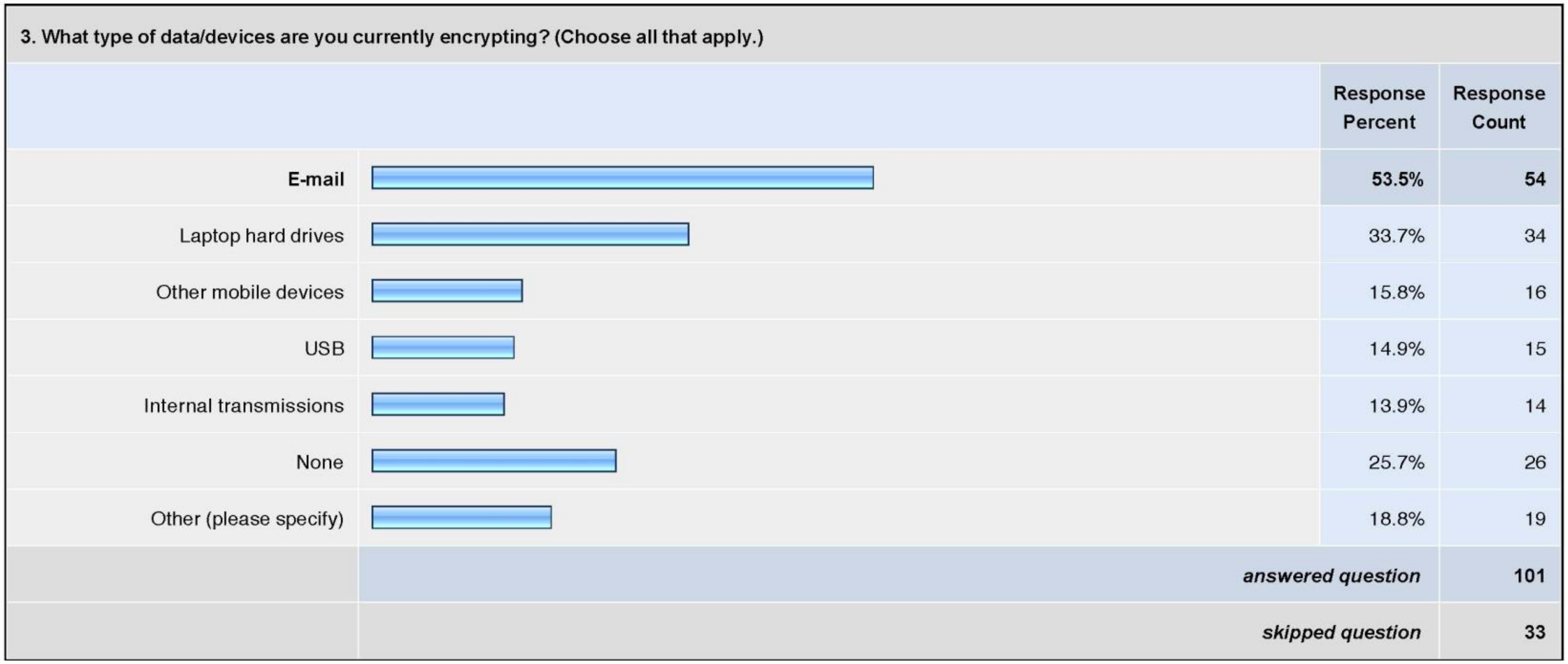
- Greater than 1/3, or 34.1%, of the responses were from organizations with less than 200 employees
- 24.2% of respondents represented organizations with more than 2001 employees
- 60% of respondents were from organizations of less than 700 employees

In reviewing the survey results below, the level of compliance for a number of specific implementation specifications varies, and a low level of compliance with some standards is evident. In presenting these results, neither the Security Networking Group nor HIPAA COW, are, in any manner, justifying or giving credence to non-compliance or support a lack of thorough or complete implementation of the regulations. We are merely presenting the results of the survey. On the contrary, one of the goals in conducting this Benchmarking Survey was to assist Security Officers and others responsible for implementation of the regulations in understanding where the gaps in compliance exist and to help in determining the reason for failure to completely implement the regulations.

The Security Networking Group also made note of the number of respondents that “skipped” certain questions. We speculated the reason respondents skipped a question was that they simply did not know the answer or that they possibly felt uncomfortable representing that their organization was, in fact, non-compliant with that particular standard. Other possible explanations certainly exist.

3.0 Survey Results

3.1 Encryption



3. What type of data/devices are you currently encrypting? (Choose all that apply.)

	Response Percent	Response Count
E-mail	**53.5%**	**54**
Laptop hard drives	33.7%	34
Other mobile devices	15.8%	16
USB	14.9%	15
Internal transmissions	13.9%	14
None	25.7%	26
Other (please specify)	18.8%	19
	answered question	**101**
	skipped question	**33**

3.1.1 Data/Results

- More than 1/2 , or 53.5%, are encrypting e-mail; 46% are not encrypting e-mail
- Only 1/3, or 33.7%, are encrypting laptops; 66% are not encrypting laptops
- Less than 1/3, or 30.7%, are encrypting USBs and other mobile devices
- More than 1/4 , or 25.7%, *are not encrypting any type* of electronic communications

3.1.2 Committee Observations

- In consideration that encryption is an “addressable” requirement, and given the responses above, the Security Networking Group deliberated the reason/s why encryption has not been implemented and identified obstacles such as budgetary limitations, difficulties or complexities in implementation, and IT departments that might not be prepared or that might not have the resources to administer the technology once implemented. It was also mentioned that some organizations were, most likely, currently implementing or testing to find adequate solutions to this problem or have a belief that comprehensively implementing encryption is nearly impossible. One explanation shared in the narrative comments, was that instead of implementing encryption to protect PHI in email transmissions, organizations have established policies that prohibit transmission of PHI in e-mail or on portable devices.

- While the actual HIPAA specification is considered ”Addressable", it by no means absolves Covered Entities from their responsibility to implement a 'reasonable and appropriate' solution to meet the standard in the regulations. In the “HIPAA Compliance Review Analysis and Summary of Results” from CMS, released late in 2008, CMS discussed the problematic areas of compliance with the HIPAA Security Rule. Specifically regarding encryption, they noted:

> *"Because of the proliferation of portable devices and media, the risk of loss or theft of ePHI has increased. Although this implementation specification is addressable, strong encryption provides additional assurances over the protection of ePHI, even in cases where portable devices are lost or stolen. The combination of CMS's recommendation in the remote use guidance, the increasing number of incidents involving lost portable devices, and the decreasing cost of encryption solutions has resulted in an environment where encryption may not be optional under the mantra of reasonable and appropriate.*"[1]

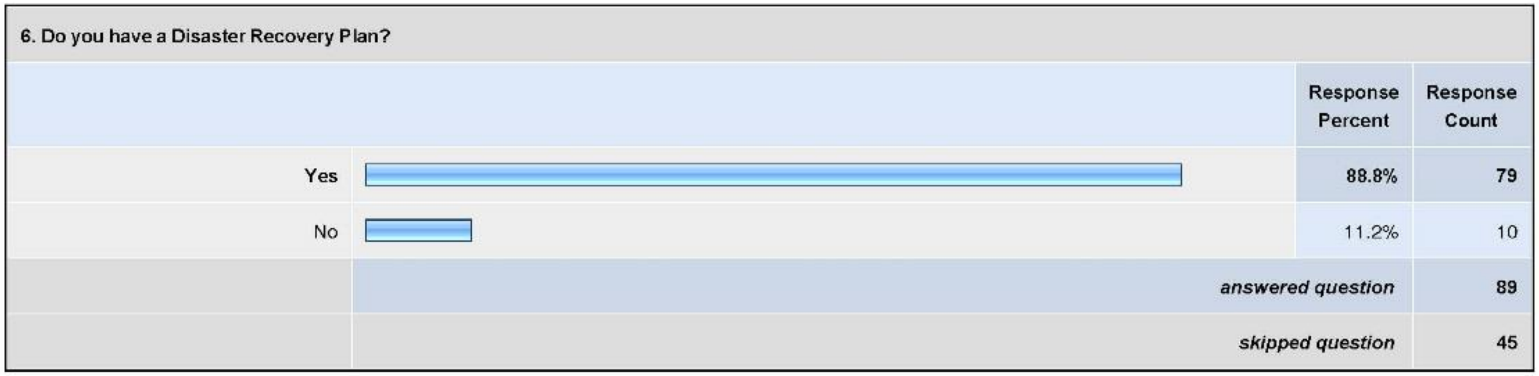
- To add to the already complicated interpretation of the rule(s), the recent HITECH Act specifies severe penalties for breaches of unsecured PHI, and further states that these penalties do not apply if data is encrypted or otherwise rendered unusable, unreadable, or indecipherable.

3.1.3 Conclusions/Recommendations

- Prior to obtaining the survey results, the Security Networking Group’s expectation was that organizations had implemented encryption techniques/solutions on more types of devices than the survey results indicated. Given the number of inexpensive, easy to implement solutions, and well-established technology, the Security Networking Group believes most organizations should be capable of encryption. There is significant risk to the security of ePHI and of regulatory scrutiny if your organization is not implementing encryption techniques/solutions.
- The CMS guidance above implies that encryption is not optional, and recent audits by the OCR, OIG, and other agencies suggest that failure to encrypt data *may* contribute to an audit failure. The Security Networking Group is concerned that simply educating users that PHI cannot be included in email messages is an effective solution.
- The Security Networking Group believes that the best encryption solutions do not rely on users to determine how to send email safely if PHI must be sent via email. Instead, the Information Technology Department (“IT”) should provide proactive solutions to users whenever possible.

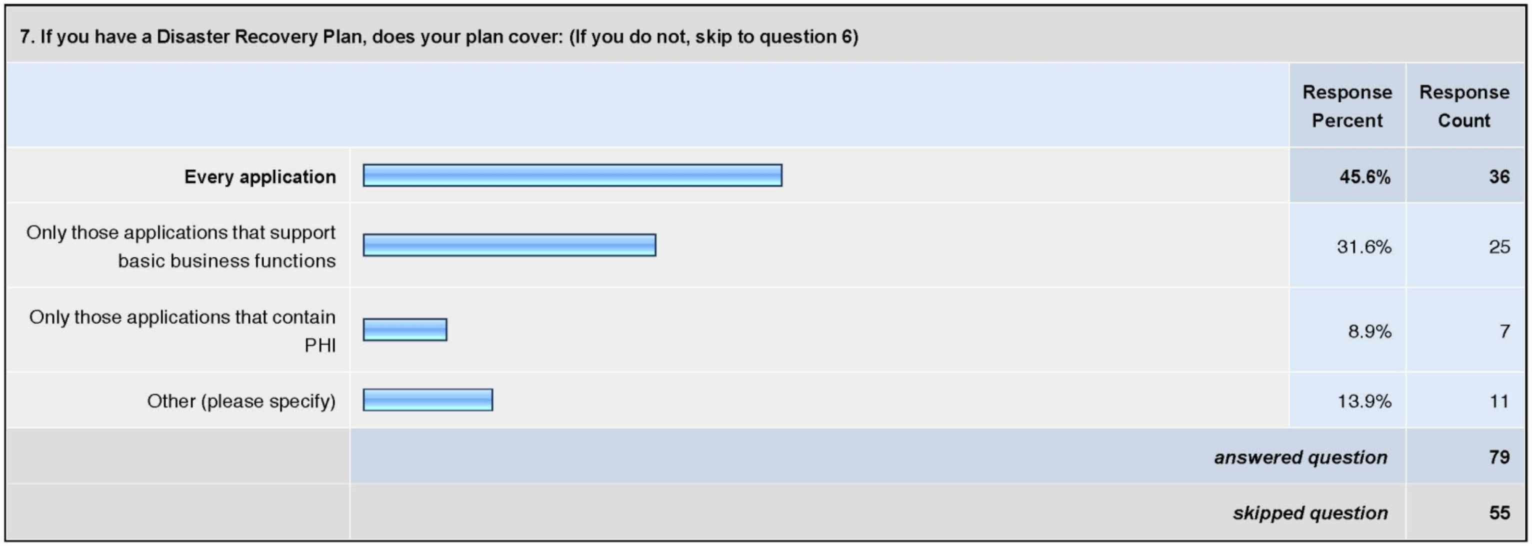
[1] HIPAA Compliance Review Analysis and Summary of Results – 2008
http://www.hhs.gov/ocr/privacy/hipaa/enforcement/cmscompliancerev08.pdf

3.2 Disaster Recovery



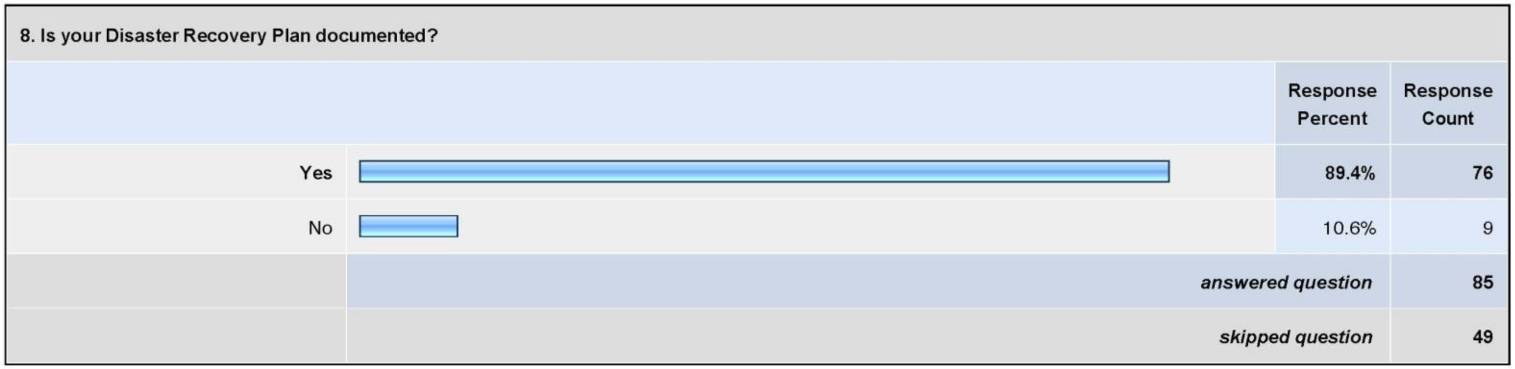
6. Do you have a Disaster Recovery Plan?

	Response Percent	Response Count
Yes	**88.8%**	**79**
No	11.2%	10
	answered question	**89**
	skipped question	**45**



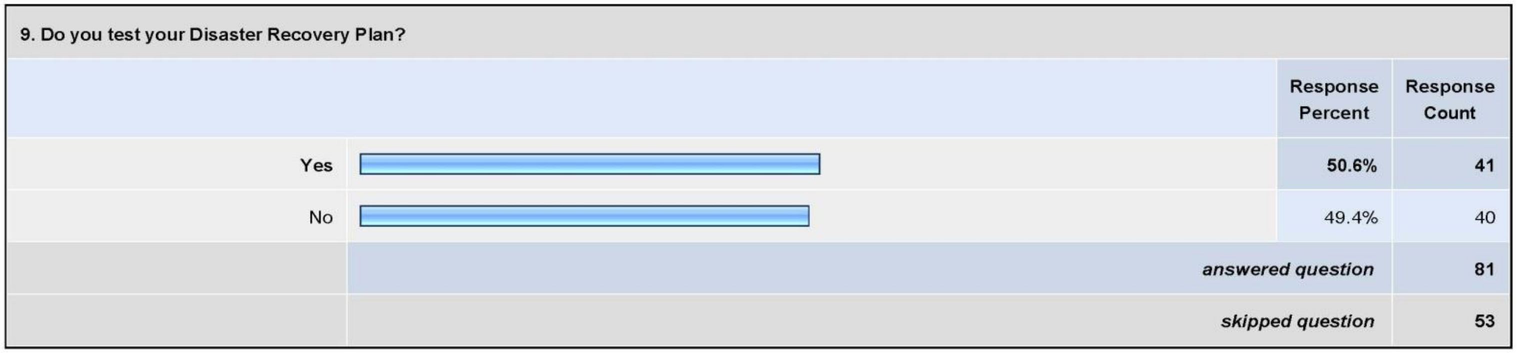
7. If you have a Disaster Recovery Plan, does your plan cover: (If you do not, skip to question 6)

	Response Percent	Response Count
Every application	**45.6%**	**36**
Only those applications that support basic business functions	31.6%	25
Only those applications that contain PHI	8.9%	7
Other (please specify)	13.9%	11
	answered question	**79**
	skipped question	**55**



8. Is your Disaster Recovery Plan documented?

	Response Percent	Response Count
Yes	89.4%	76
No	10.6%	9
answered question		85
skipped question		49



9. Do you test your Disaster Recovery Plan?

	Response Percent	Response Count
Yes	50.6%	41
No	49.4%	40
answered question		81
skipped question		53

3.2.1 Data/Results

- 88.8%, or the majority of respondents that answered the question, have a Disaster Recovery Plan
- Close to 1/2 , or 45.6%, state their Disaster Recovery Plan covers every application
- Almost 1/3, or 31.6%, indicated their Disaster Recovery Plan covers only those applications that support basic business functions
- The majority, or 89.4%, state their Disaster Recovery Plan is *documented*.
- Almost exactly 1/2 , or 50.6%, *test* their Disaster Recovery Plan
- 34% of respondents skipped the question
- Of those that answered the question and provided narrative comments as to how often they test their Disaster Recovery Plan, the responses varied from monthly to every other year, with the majority of respondents indicating annual testing.

3.2.2 Committee Observations

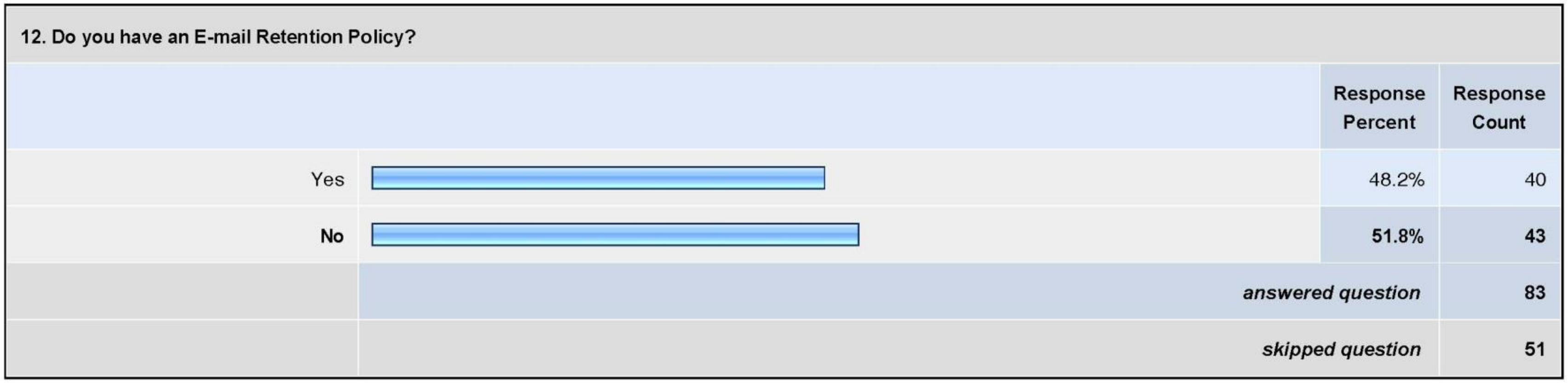
- Since The Joint Commission for Accreditation of Healthcare Organizations ("The Joint Commission") requires a disaster plan that is tested, the Security Networking Group wondered if there was confusion between the plan required by The Joint Commission and a data disaster recovery plan.
- About half of the respondents stated that their plan was tested. Again there may have been confusion over the required Joint Commission testing and testing of a data disaster recovery plan.
- Even though 88.8% of respondents indicated they have a Disaster Recovery Plan, one of Security Networking Group's concerns is that most are really disaster "response" or business continuity plans that have little to do with "recovery" from a data disaster, in a situation such as a computer room failure. Disaster "recovery" can be defined as getting systems back up and running. Business continuity (or patient care continuity) is keeping as much necessary data available whenever needed, which is much easier than having to completely recover systems.
- One of the challenges with meeting the intent of this requirement is that the environment is dynamic and becoming continually more complex with the addition of new systems and applications. Therefore, the processes for disaster recovery must be persistently enhanced.
- Security Networking Group also questioned if many organizations are actually making use of their Disaster Recovery Plan.
- The Security Networking Group acknowledged that it can be very difficult to obtain the resources to address this standard, e.g., IT is often under great productivity pressures and perhaps must choose between implementing a new clinical application or spending time and resources addressing Disaster Recovery - an unknown or potential issue that has no impact on day-to-day operations.

3.2.3 Conclusions/Recommendations

- Over the longer term health care organizations need to look at more than just Disaster Recovery. A weather disaster like Hurricane Katrina or a tornado is a disaster for both patients and the means to access data stored about them. However, more often a computer system disaster, like a server room failure, may not be at all related to delivering patient care. In all cases health care entities need to focus on continuity of care. In a situation requiring unscheduled downtime of a system, for instance, patient care employees generally reference established downtime policies and procedures so not to interrupt patient care.
- The process of developing and implementing a Disaster Recovery Plan is daunting so it is critical for organizations that are not currently meeting this requirement to get started. The Security Networking Group recommends beginning by prioritizing applications, e.g., applications containing PHI might be the first priority, communication systems might be the next priority, etc. Next IT might *document* steps necessary to bring each application back up once it is down and consideration can be given to conducting a "criticality analysis" with input from business leaders, weighing priority and required resources.
- Testing of the Disaster Recovery Plan can then be conducted based upon priority levels, and should also include bringing the entire system back up from scratch.
- This HIPAA Security Rule standard might be one area in which Covered Entities may want to consider working with an external vendor with this specific expertise.

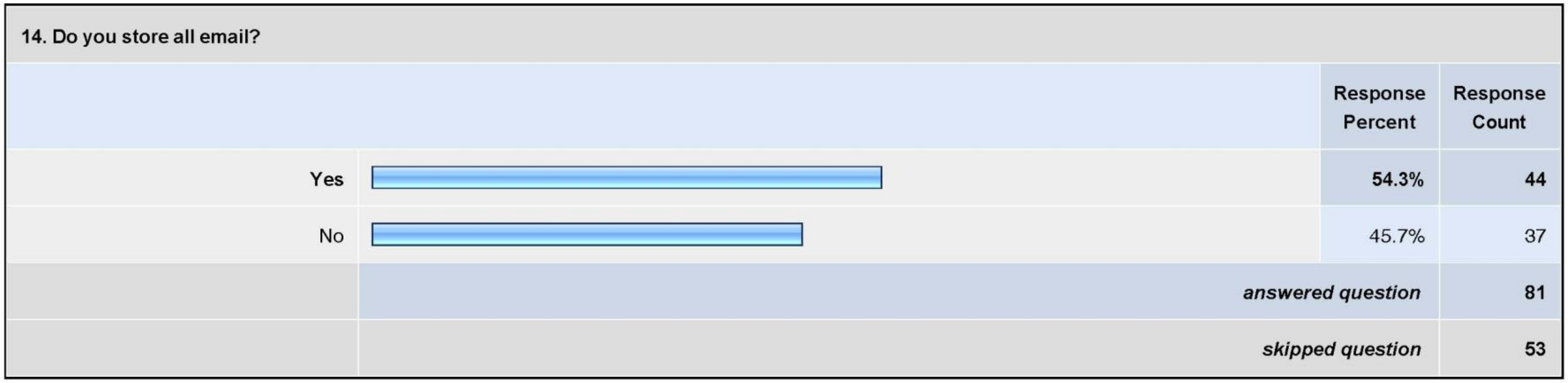
- Understanding the implications of disaster recovery should be a component of the application implementation process. The Security Networking Group recommends attempting to build into each system or application an individual recovery plan taking into account how long it takes to replace it in its entirely, i.e., all the hardware and software.

3.3 E-mail Retention



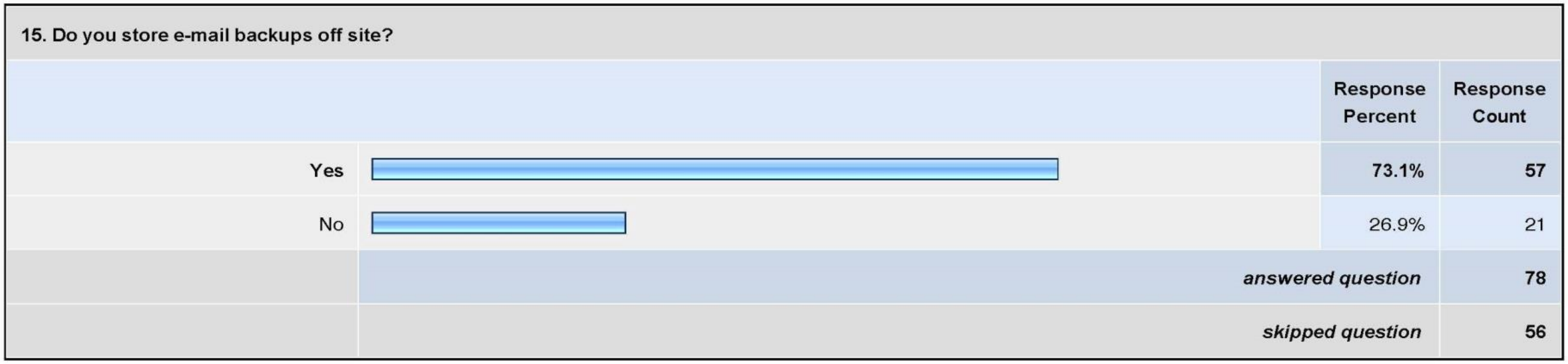
12. Do you have an E-mail Retention Policy?

		Response Percent	Response Count
Yes		48.2%	40
No		**51.8%**	**43**
		answered question	**83**
		skipped question	**51**



14. Do you store all email?

		Response Percent	Response Count
Yes		**54.3%**	**44**
No		45.7%	37
		answered question	**81**
		skipped question	**53**



15. Do you store e-mail backups off site?

	Response Percent	Response Count
Yes	**73.1%**	**57**
No	26.9%	21
answered question		**78**
skipped question		**56**

3.3.1 Data/Results

- Almost 1/2, or 48.2%, have an E-mail Retention Policy
- Just more than 1/2 , or 54.3%, store all e-mail; 45.7% do not store all e-mail
- 73.1% store e-mail back-ups off-site

3.3.2 Committee Observations

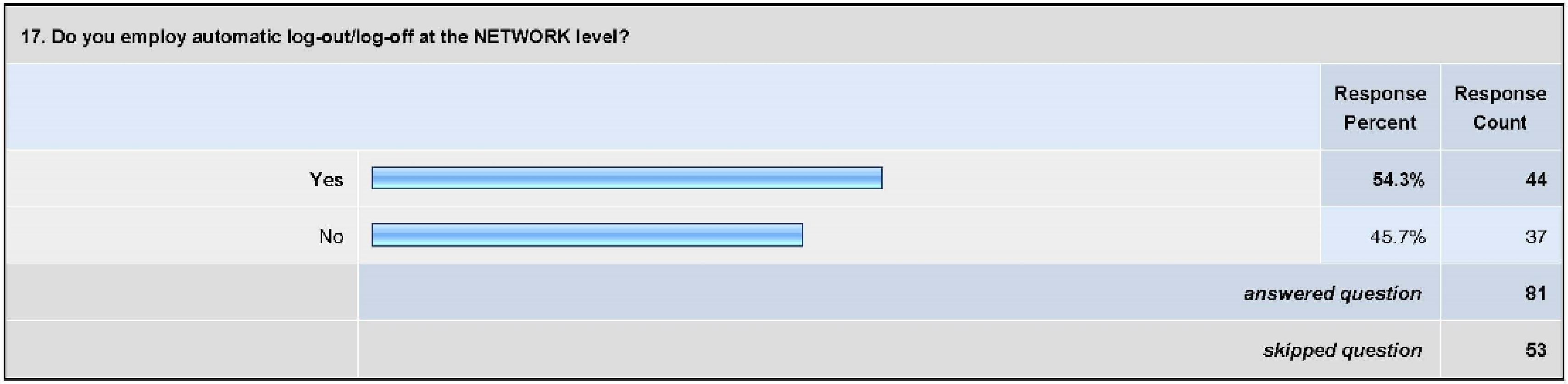
- Without a policy, in response to a legal discovery request, what would you produce? What can be discarded and what must be retained?
- The emerging laws and guidances regarding e-discovery must be continually re-evaluated.
- Once it is determined that email will be retained, further consideration must be given to “how” it is going to be retained.

3.3.3 Conclusions/Recommendations

- An organization’s document retention policy/schedule should be based upon the data elements, not upon the medium, i.e., the types of data being managed should be classified and should dictate the time period and method for retention, independent of whether the data is on paper, imaged, emailed, etc. The medium or format should not dictate the period of retention.
- Training to ensure clear understanding of the document retention schedule is critical.
- Auditing must be conducted to verify that documents are being retained for the established time period and to ensure that documents are *not* being retained longer than established in policy.

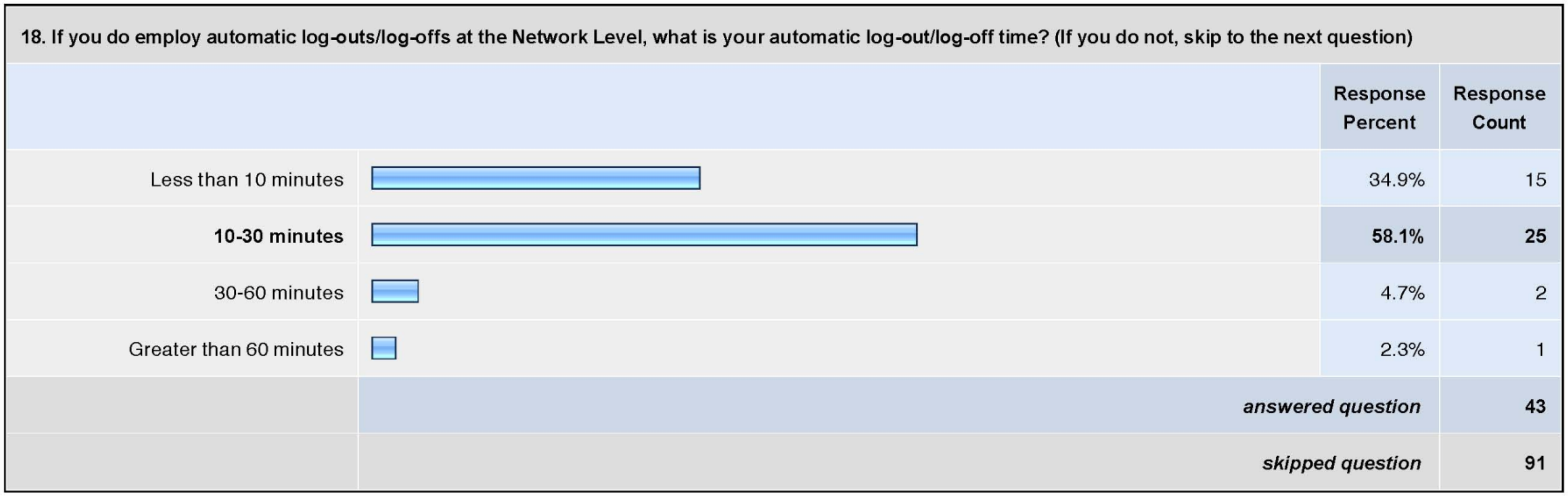
3.4 Automatic Log-out/off

(Questions regarding automatic log-out/off were separated into log-out/off at the network level and log-out/off at the application level.)



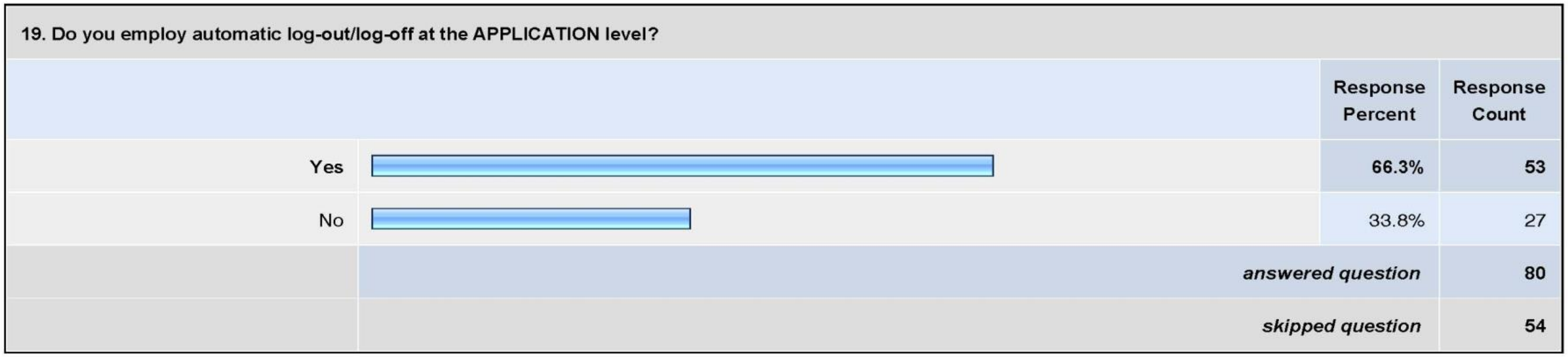
17. Do you employ automatic log-out/log-off at the NETWORK level?

	Response Percent	Response Count
Yes	**54.3%**	**44**
No	45.7%	37
	answered question	**81**
	skipped question	**53**



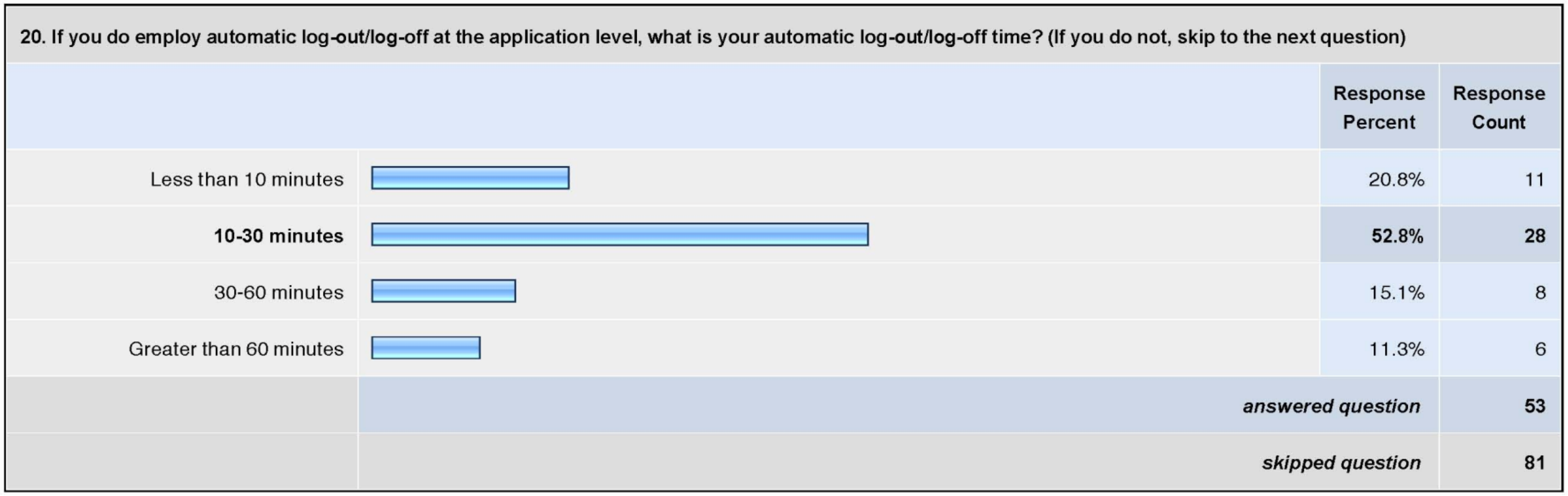
18. If you do employ automatic log-outs/log-offs at the Network Level, what is your automatic log-out/log-off time? (If you do not, skip to the next question)

	Response Percent	Response Count
Less than 10 minutes	34.9%	15
10-30 minutes	**58.1%**	**25**
30-60 minutes	4.7%	2
Greater than 60 minutes	2.3%	1
	answered question	**43**
	skipped question	**91**



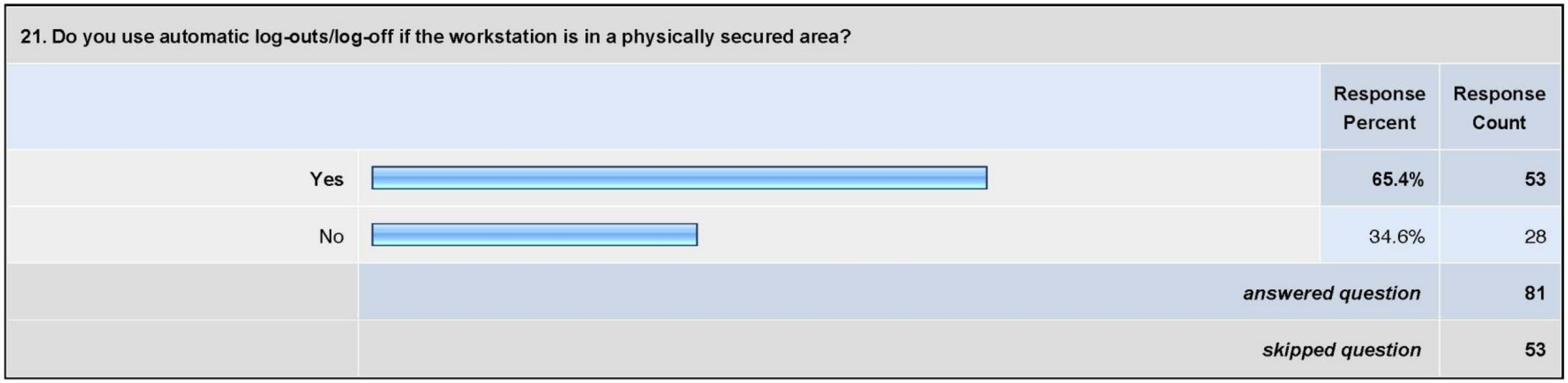
19. Do you employ automatic log-out/log-off at the APPLICATION level?

		Response Percent	Response Count
Yes		**66.3%**	**53**
No		33.8%	27
		answered question	**80**
		skipped question	**54**



20. If you do employ automatic log-out/log-off at the application level, what is your automatic log-out/log-off time? (If you do not, skip to the next question)

		Response Percent	Response Count
Less than 10 minutes		20.8%	11
10-30 minutes		**52.8%**	**28**
30-60 minutes		15.1%	8
Greater than 60 minutes		11.3%	6
		answered question	**53**
		skipped question	**81**



21. Do you use automatic log-outs/log-off if the workstation is in a physically secured area?

	Response Percent	Response Count
Yes	**65.4%**	**53**
No	34.6%	28
answered question		**81**
skipped question		**53**

3.4.1 Data/Results

Network Level

- Just over 1/2, or 54.3%, employ automatic log-out at the *network* level

- Of those who employ automatic log-out at the *network* level:
  - More than half, or 58.1%, have implemented log-out times of 10-30 minutes
  - Another approximately 1/3, 34.9%, implemented log-outs of less than 10 minutes
  - ***Which indicates that 93% require log-out times at the network level to be less than 30 minutes***

- Only 7% have implemented log-out times at the *network* level of greater than 30 minutes

Application Level

- About 2/3, or 66.3%, employ log-outs at the *application* level

- Of those who employ automatic log-outs at the *application level*:
  - More than half, or 52.8%, have implemented log-out times of 10-30 minutes
  - Another 20% have implemented log-out times of less than 10 minutes
  - 1/4, or 26.4%, have implemented log-out times at the *application* level of more than 30 minutes
  - ***Which indicates that 73.6% require lot-out times at the application level to be less than 30 minutes***

Physically Secured

- If work stations are in a physically secured area, approximately 2/3, or 65.4%, still require an automatic log-out; inversely about 1/3, or 34.6%, do not use automatic log-outs if a workstation is in a physically secured area

3.4.2 Committee Observations

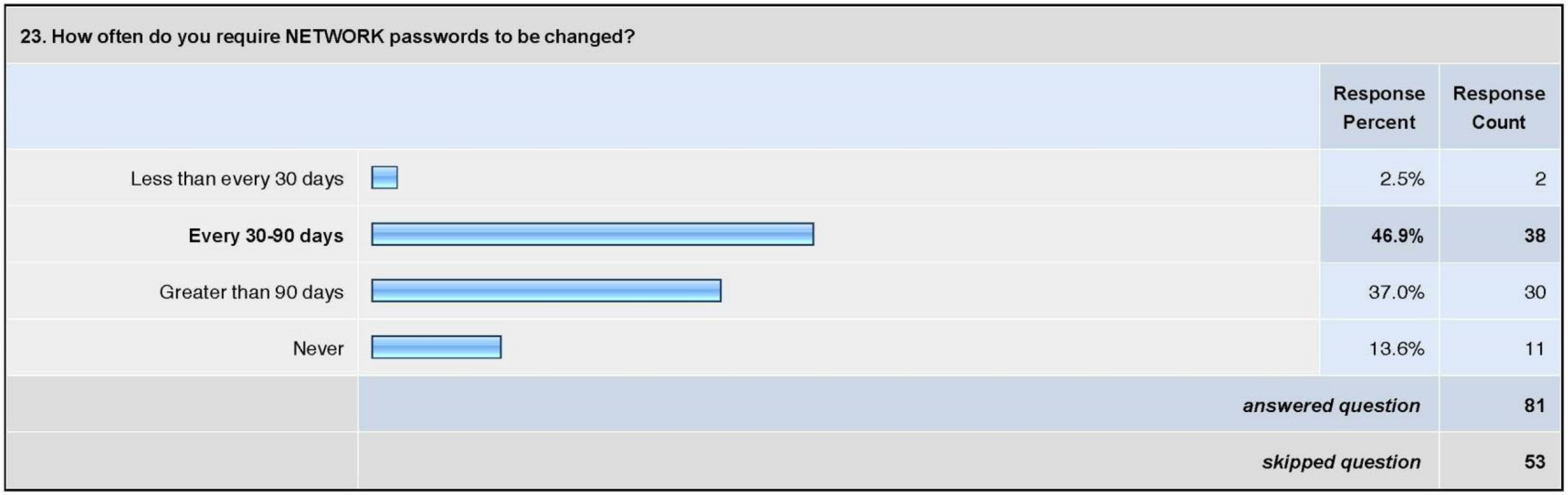
- The results of this survey seem to indicate that most organizations establish log-out times at either the network or application level of less than 30 minutes.
- Even if work stations are considered to be in physically secured locations, most organizations still require automatic log-outs.
- The ongoing challenge of “auto logout/logoff” appears to be finding the best fit between ensuring security and the impact on the usability of a system. These decisions may vary when comparing ambulatory and inpatient settings. Frequently, the “time out” decision for a vendor is set at the system level and flexibility for varying environments is not supported.
- As systems continue on a path of integration, leveraging ability to carry context (user, patient) from system to system and application to application, the focus of appropriately securing workstations will continue to be a topic of discussion. This will be particularly true as systems leave the bounds of the “local network” and reach into community based services, systems and data bases.

3.4.3 Conclusions/Recommendations

- Management of multiple time out parameters, across various systems may be mitigated through the use of a “network level” setting. Appropriate steps should be taken to ensure that logout at a network level does not negatively impact workflow for other workstation and application users in the same environment.
- While “auto logout/logoff” is a good security safety net, it should not be implemented without supporting the workflow practice of users “logging off” or otherwise “securing” a given application or network connection. This personal accountability is critical to appropriate user accountability. It would be interesting to conduct a study of the number of “open” applications when a network “auto logout/logoff” occurs.
- It is perhaps ideal that all institutions implement both application level account management and network level services. Security risks will also be minimized by setting “auto logout/logoff” and monitoring the frequency of “auto logout/logoff” occurrences. Policies should be established to define what determines a given environment to be “secure” and therefore subject to a “longer” or “not implemented” “auto logout/logoff”.

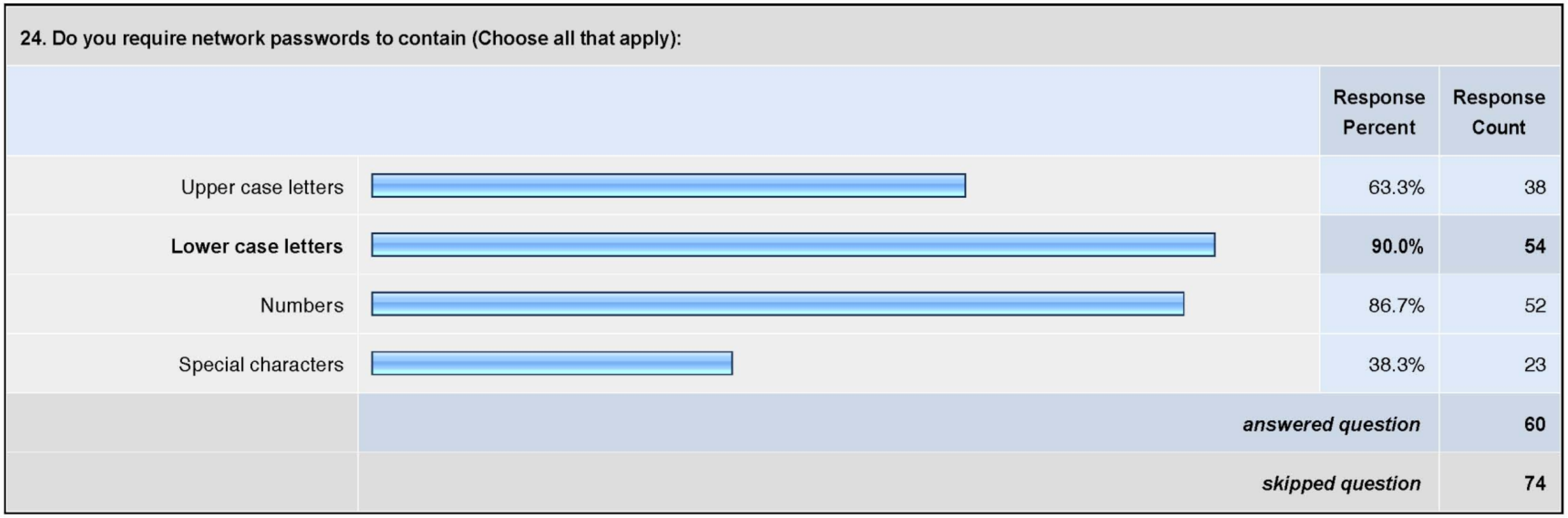
3.5 Password Management

(Questions regarding password management were categorized as either at the network level or at the application level.)



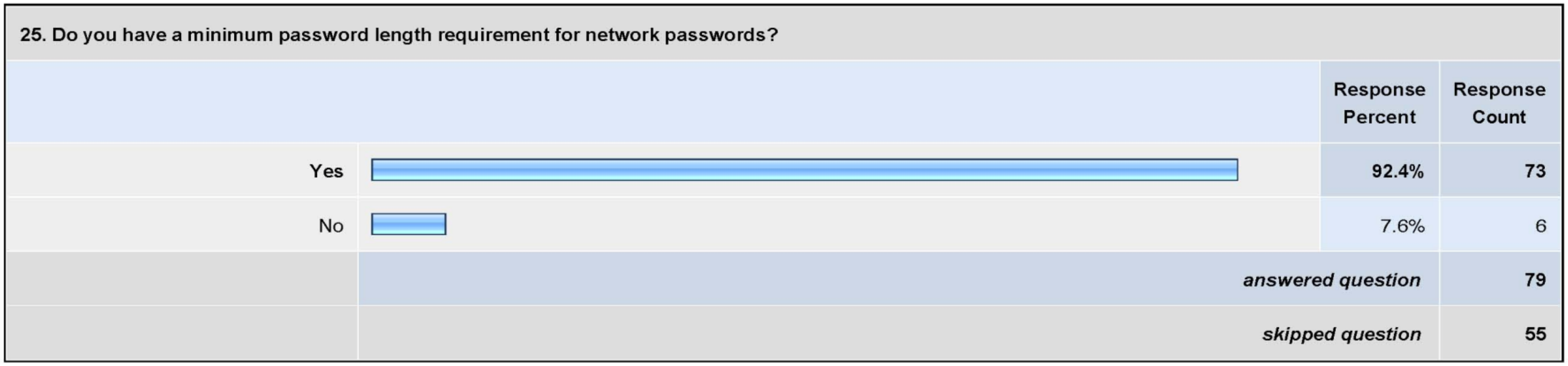
23. How often do you require NETWORK passwords to be changed?

		Response Percent	Response Count
Less than every 30 days		2.5%	2
Every 30-90 days		**46.9%**	**38**
Greater than 90 days		37.0%	30
Never		13.6%	11
	answered question		**81**
	skipped question		**53**



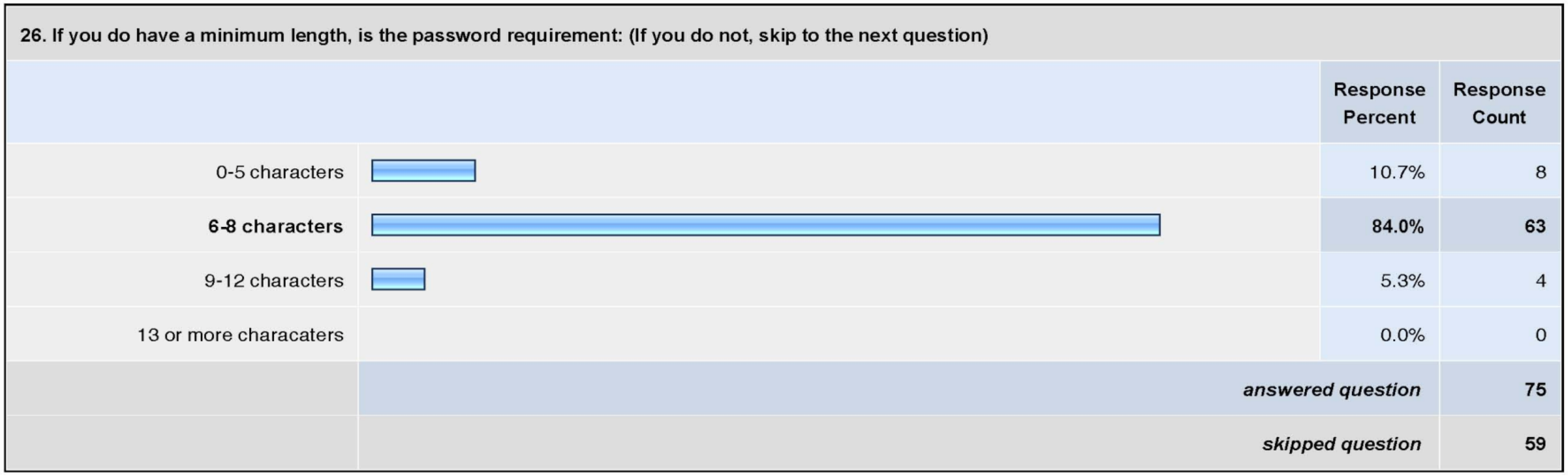
24. Do you require network passwords to contain (Choose all that apply):

		Response Percent	Response Count
Upper case letters		63.3%	38
Lower case letters		**90.0%**	**54**
Numbers		86.7%	52
Special characters		38.3%	23
	answered question		**60**
	skipped question		**74**



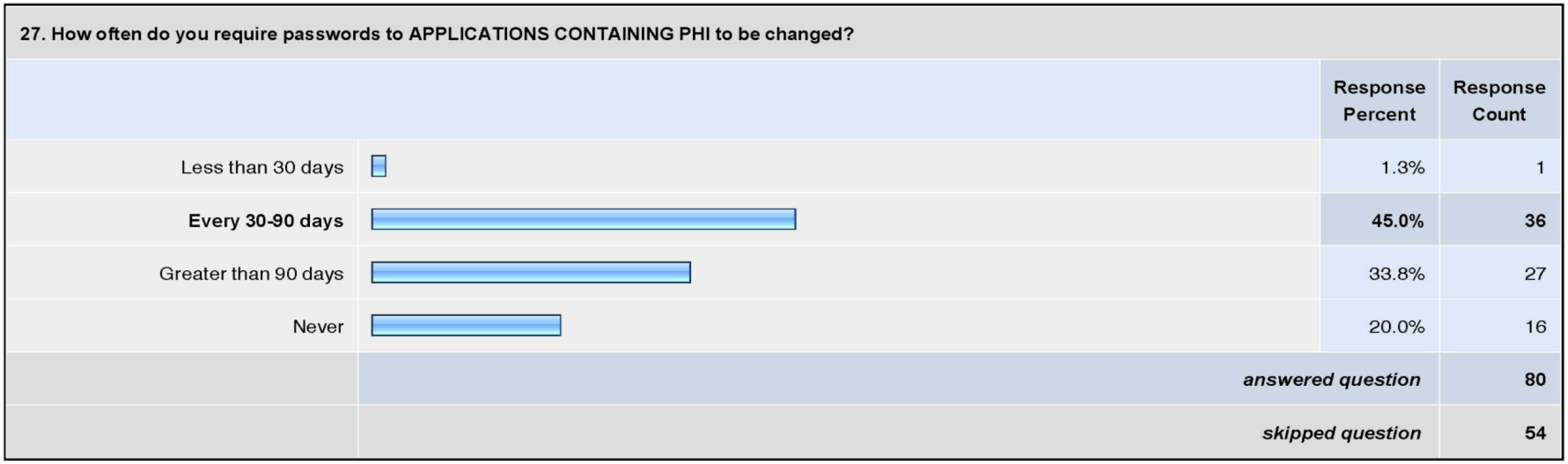
25. Do you have a minimum password length requirement for network passwords?

		Response Percent	Response Count
Yes		**92.4%**	**73**
No		7.6%	6
	answered question		**79**
	skipped question		**55**



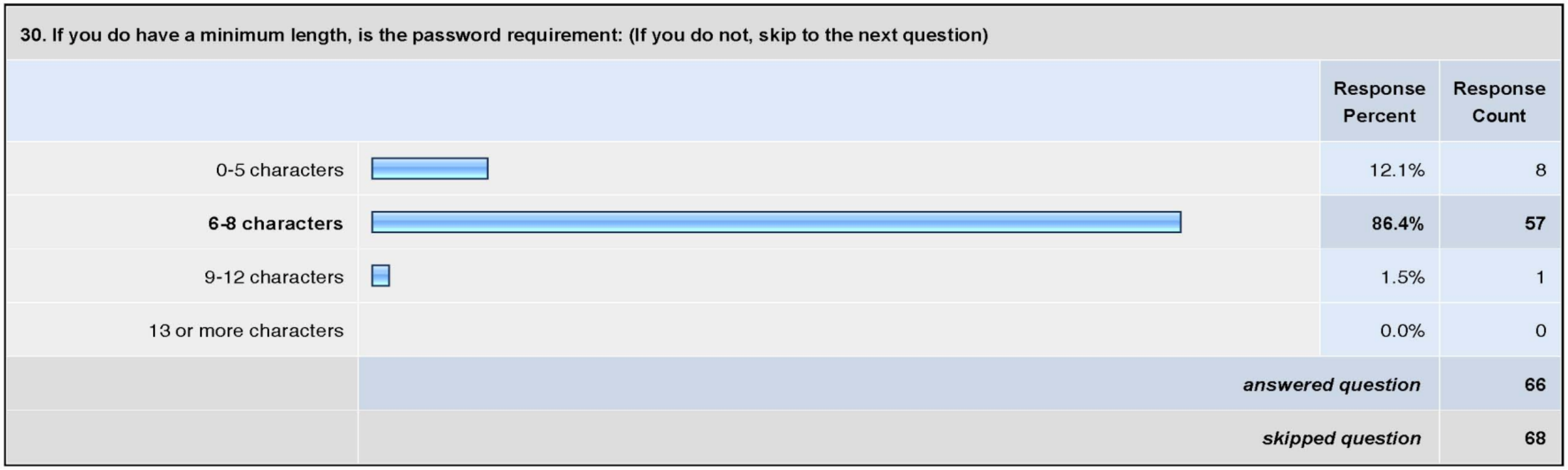
26. If you do have a minimum length, is the password requirement: (If you do not, skip to the next question)

		Response Percent	Response Count
0-5 characters		10.7%	8
6-8 characters		**84.0%**	**63**
9-12 characters		5.3%	4
13 or more characaters		0.0%	0
	answered question		**75**
	skipped question		**59**



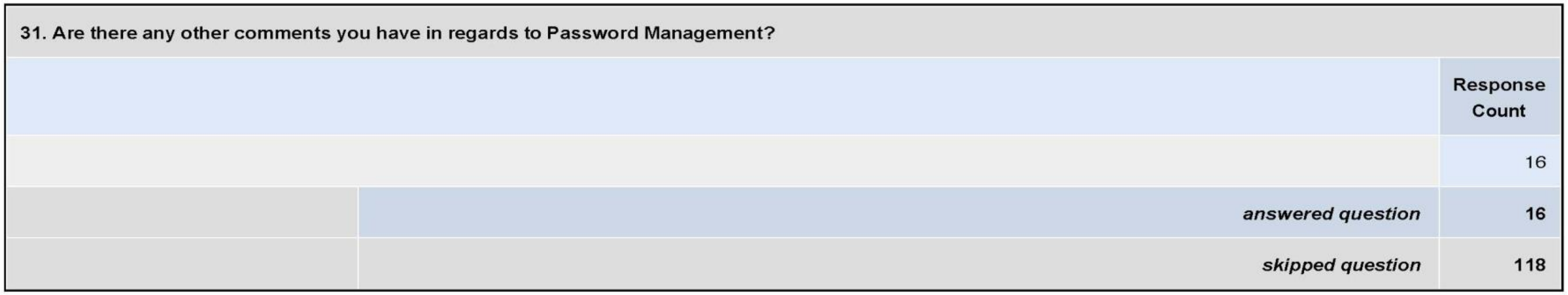
27. How often do you require passwords to APPLICATIONS CONTAINING PHI to be changed?

	Response Percent	Response Count
Less than 30 days	1.3%	1
Every 30-90 days	**45.0%**	**36**
Greater than 90 days	33.8%	27
Never	20.0%	16
	answered question	**80**
	skipped question	**54**



30. If you do have a minimum length, is the password requirement: (If you do not, skip to the next question)

	Response Percent	Response Count
0-5 characters	12.1%	8
6-8 characters	**86.4%**	**57**
9-12 characters	1.5%	1
13 or more characters	0.0%	0
	answered question	**66**
	skipped question	**68**



31. Are there any other comments you have in regards to Password Management?

		Response Count
		16
	answered question	**16**
	skipped question	**118**

3.5.1 Data/Results

Network Passwords

- Almost 1/2, or 46.9%, require *network* passwords to be changed every 30-90 days; more than 1/3, or 37%, only require passwords to be changed after more than 90 days; 13.6% *never* require passwords to be changed
    - **Which indicates that 83.9% of respondents require network passwords to be changed after more than 90 days**
- The vast majority, or 92.4%, have a minimum password length for passwords at the *network* level:
    - 84% require passwords to contain 6-8 characters
    - Another 5.3% require network passwords to contain 9-12 characters
    - **Which indicates that 89.3% require passwords to be at least 6 characters in length**

Application Passwords

- Almost 1/2, or 45%, require passwords to *applications that contain PHI* to be changed every 30-90 days; another 1/3, or 33.8% require passwords to be changed after more than 90 days; 20% *never* require passwords to be changed at the application level
    - **Which indicates that 78.8% of respondents require passwords to *applications that contain PHI* to be changed after more than 90 days**
- The vast majority, or 86.1%, have a minimum password length for passwords at the *application* level:
    - 86.4% require passwords to contain 6-8 characters
    - 1.5% require application passwords to contain 9-12 characters
    - **Which indicates that 87.9% require passwords to be at least 6 characters in length**

3.5.2 Committee Observations

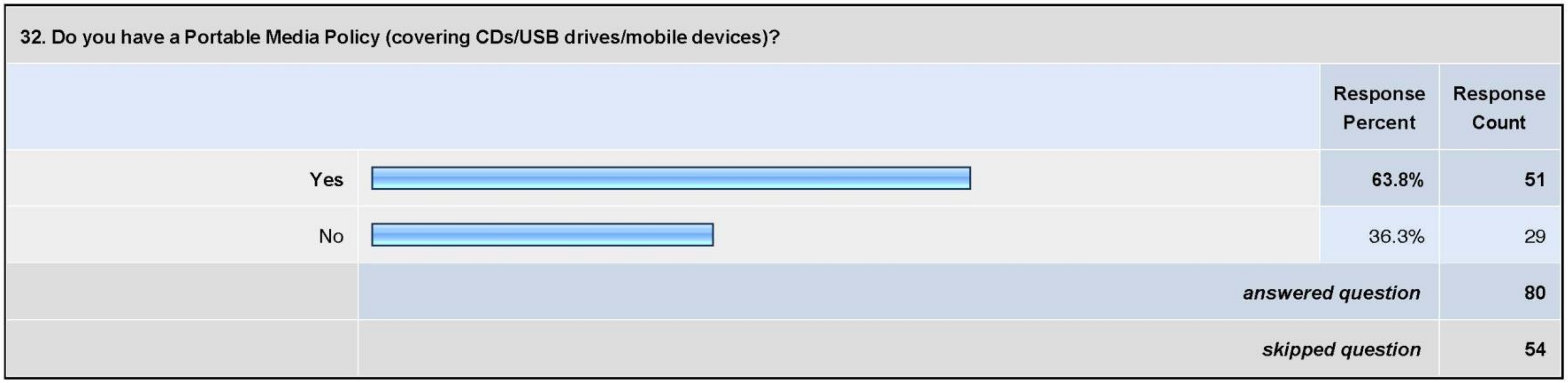
- There does not appear to be a clear agreement regarding how often either network or application passwords are changed, although the majority seems to require passwords to be changed after more than 90 days.

- There does not appear to be a clear agreement regarding password length at either the network or application level, although the results seem to indicate that most organizations require passwords to be at least 6 characters in length
- Password strength and policy on frequency of change presents the challenge of balancing security and ease of use. This is further compounded by the multivariate environment of password strength, number of passwords, synchronization of password change times, and user frustration resulting in creative solutions to “remembering” their passwords (look under the mouse pad or on the back of ID badge).
- While security experts would encourage complex (8 characters minimum, upper and lower case, numbers and special characters), the challenge of users logging into systems 50 or more times in a shift is a sobering reality to these recommendations. As with “auto log out/off”, the workflow of passwords and user access needs close scrutiny. This may be further compounded by the type of workstations and the clinical work space in which a given individual works.
- Other options besides passwords will eventually arise when there are advances in context management for more “automated” identification and authentication processes that become affordable to allow implementation across thousands of users and hundreds of workstations. For example, biometric identification, combined with proximity enabled identification badges, implemented in a way that recognizes the constraints and complexities of workspace with latex gloves, and various infection control requirements cannot be far away.
- Other considerations:
    - Are the users allowed to determine how frequently their password is changed?
    - Are password requirements for applications, dependent upon the application?

3.5.3 Conclusions/Recommendations

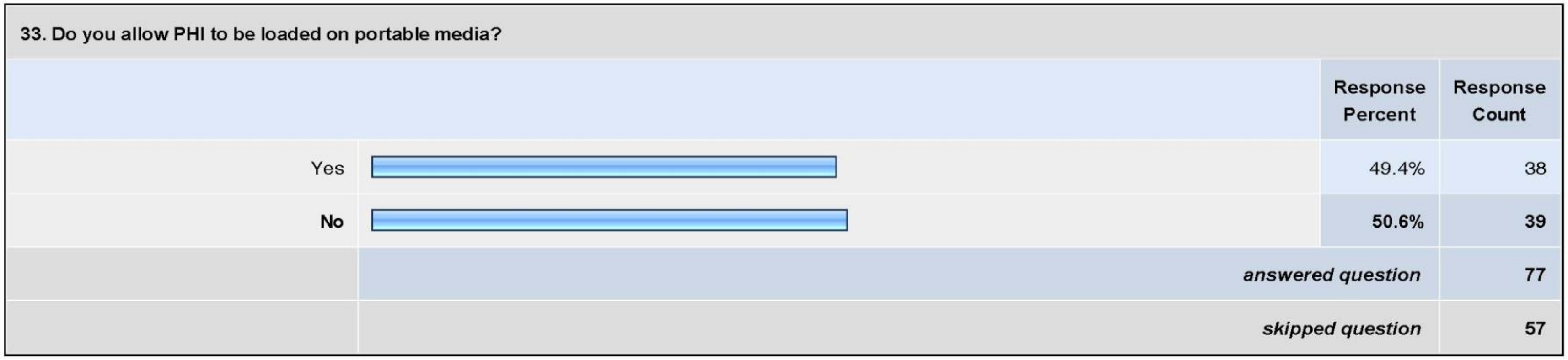
- It is the Security Networking Group’s recommendation that all institutions implement strong identification and authentication processes:
    - Passwords should be a minimum of 6, preferably 8, characters long
    - Passwords should be composed of upper and lower case letters and at least one number and one special character
    - Full words, significant dates, user IDs, and names should not be allowed as passwords
- The Security Networking Group recommends that passwords are required to be changed at least every 90 days.
- Additionally, it is suggested that some level of automated history be maintained so that two passwords are not alternated each 180 days.
- Further it is proposed that users have the ability to change their passwords “on demand” to enable alignment of multiple systems password change cycles.

3.6 Portable Media



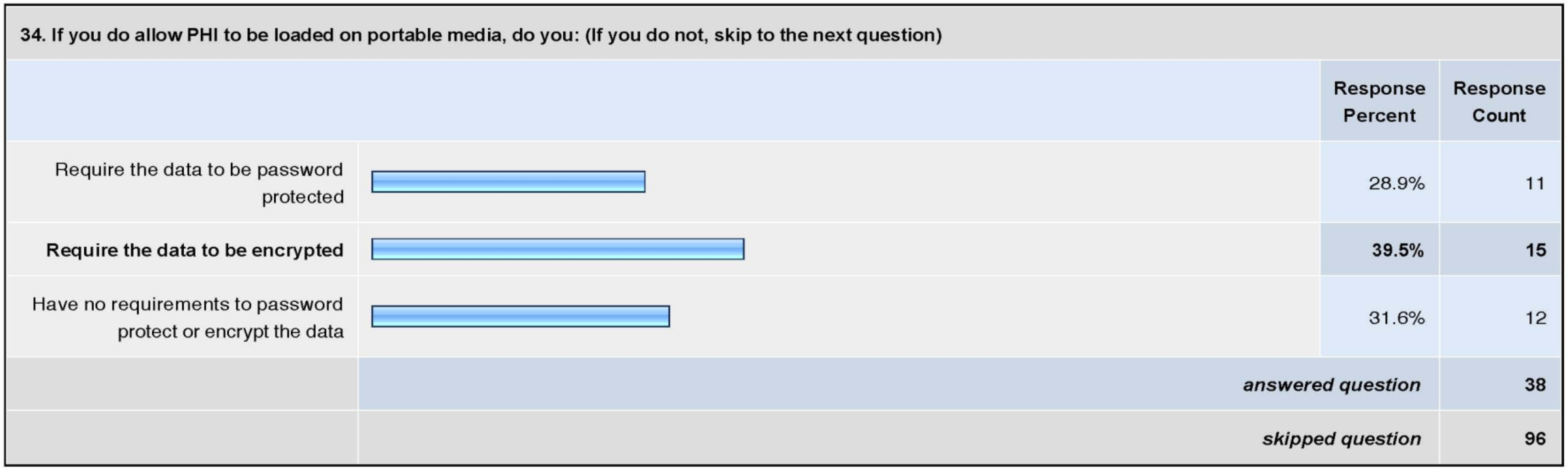
32. Do you have a Portable Media Policy (covering CDs/USB drives/mobile devices)?

	Response Percent	Response Count
Yes	63.8%	51
No	36.3%	29
answered question		80
skipped question		54



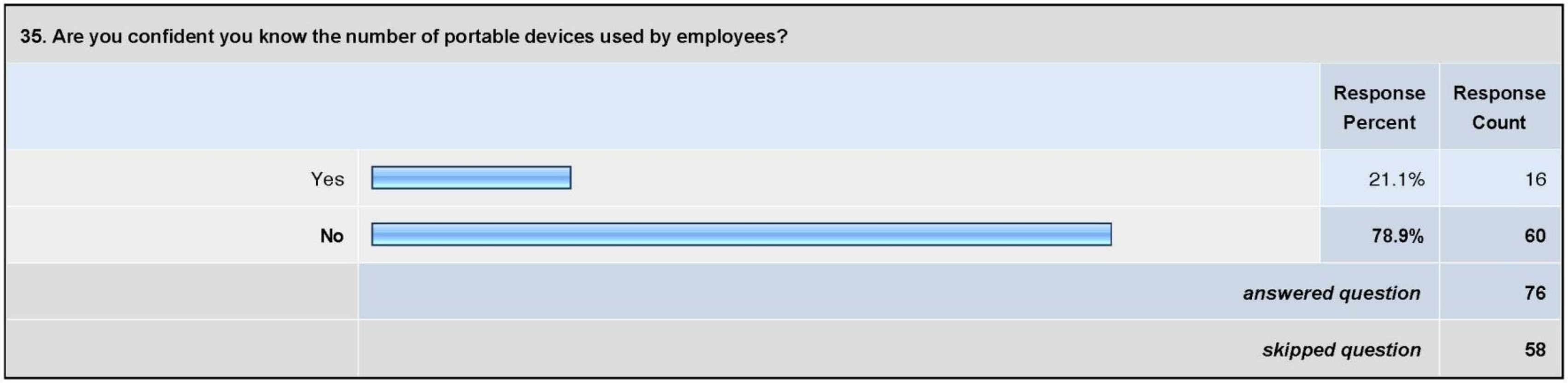
33. Do you allow PHI to be loaded on portable media?

	Response Percent	Response Count
Yes	49.4%	38
No	50.6%	39
answered question		77
skipped question		57



34. If you do allow PHI to be loaded on portable media, do you: (If you do not, skip to the next question)

		Response Percent	Response Count
Require the data to be password protected		28.9%	11
Require the data to be encrypted		**39.5%**	**15**
Have no requirements to password protect or encrypt the data		31.6%	12
	answered question		38
	skipped question		96



35. Are you confident you know the number of portable devices used by employees?

		Response Percent	Response Count
Yes		21.1%	16
No		**78.9%**	**60**
	answered question		76
	skipped question		58

3.6.1 Data/Results

- Just less than 2/3, or 63.8%, indicate they have a policy covering portable/mobile devices; another approximately 1/3, or 36.3%, do not have a policy addressing portable media
- 1/2 , or 50.6%, state it is the policy of their organization that PHI cannot be loaded on portable media
- Approximately 1/2 , or 49.4%, allow PHI to be loaded on or transmitted through portable/mobile devices
- Of those who allow PHI to be loaded on portable media, more than 2/3, or 68.4%, require the data to be password protected or encrypted, which means the other 1/3, 31.6%, have no protections in place

- More than 3/4 , 78.9%, indicate they are not confident they know the number of portable devices used by their employees; less than 1/4, or 21.2%, are confident they know the number of portable devices used by employees
- 72% of those who took the survey did not answer this question

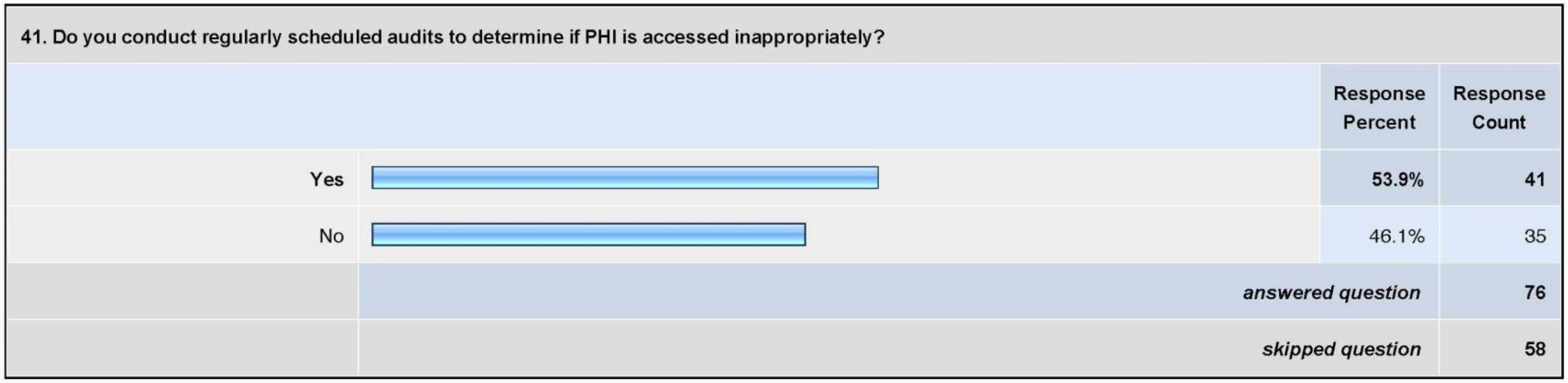
3.6.2 <u>Committee Observations</u>

- Portable media containing PHI has triggered many of the initial complaints to federal agencies resulting in investigations. (See the discussion and reference in 3.1.2 above.)
- If your policy states that PHI cannot be loaded on portable media, how do you audit or enforce this?
- For the 21.2% who believe they do know the number of portable devises being used, how do you monitor and enforce this?
- The Security Networking Group was very concerned about the finding that almost 1/2 of the organizations surveyed indicate they allow PHI to be loaded on or transmitted through portable media but 1/3 of those do not appear to have any security measures in place to protect PHI.
- Does encrypting a laptop at least partially solve this problem?

3.6.3 <u>Conclusions/Recommendations</u>

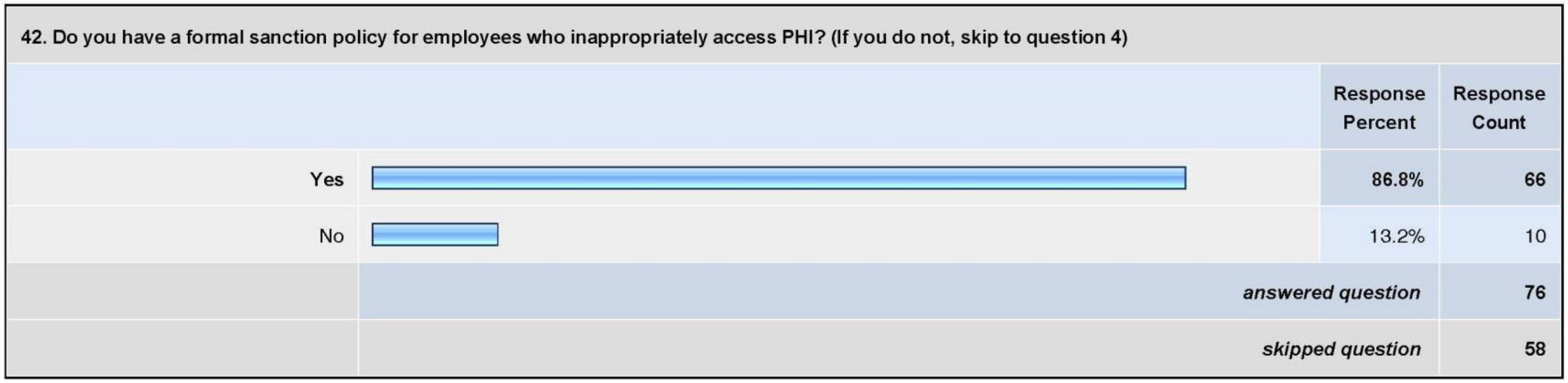
- One approach to the problem with portable devices that the Security Networking Group contemplated was to avoid instituting a policy because the organization was not sure how to enforce it. However, we still recommend having a written policy in place to hold employees accountable and to help protect the organization from individual’s wrong-doing.
- Security awareness and training for all employees regarding portable devises is absolutely critical to protecting the confidentiality and integrity of PHI. It if further recommended that language regarding protecting PHI that may be contained on any portable device is included in a training attestation.

3.7 Auditing



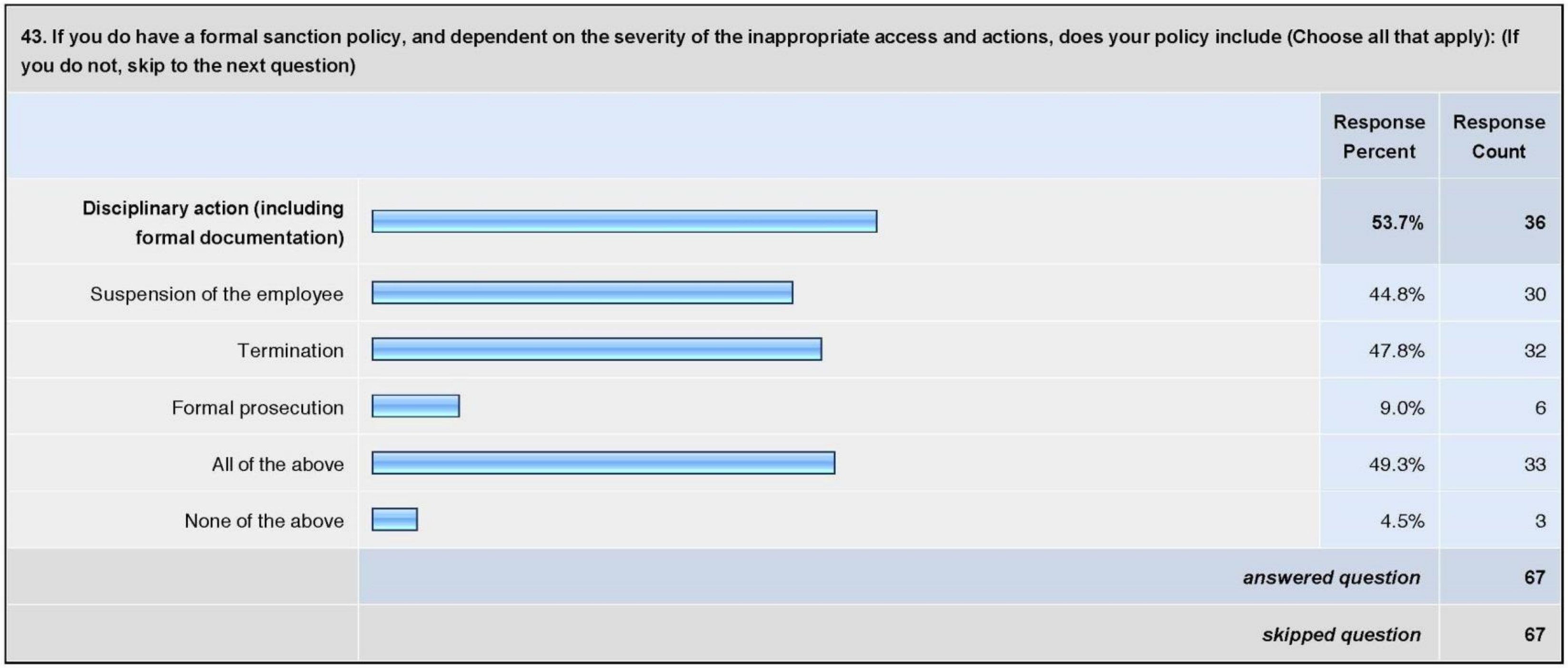
41. Do you conduct regularly scheduled audits to determine if PHI is accessed inappropriately?

		Response Percent	Response Count
Yes		**53.9%**	**41**
No		46.1%	35
		answered question	**76**
		skipped question	**58**



42. Do you have a formal sanction policy for employees who inappropriately access PHI? (If you do not, skip to question 4)

	Response Percent	Response Count
Yes	**86.8%**	**66**
No	13.2%	10
	answered question	**76**
	skipped question	**58**



43. If you do have a formal sanction policy, and dependent on the severity of the inappropriate access and actions, does your policy include (Choose all that apply): (If you do not, skip to the next question)

	Response Percent	Response Count
Disciplinary action (including formal documentation)	**53.7%**	**36**
Suspension of the employee	44.8%	30
Termination	47.8%	32
Formal prosecution	9.0%	6
All of the above	49.3%	33
None of the above	4.5%	3
	answered question	**67**
	skipped question	**67**

3.7.1 <u>Data/Results</u>

- A little more than 1/2, or 53.9%, responded that they conduct regularly scheduled audits to determine if PHI is accessed inappropriately; almost 1/2, or 46.1%, do not conduct this type of auditing

- The vast majority, 86.8%, indicate they have a formal sanction policy for employees who inappropriately access PHI
- Dependent on the severity of the inappropriate access, these sanction policies include the following types of discipline:
    - 53.7% formal, documented discipline
    - 47.8% termination of the employee
    - 44.8% suspension of the employee
    - 9% formal prosecution
    - 49.3% all of the above
    - 4.5% utilize none of the above sanctions

3.7.2 Committee Observations

- The HIPAA COW Security Networking Group Committee was not surprised by these results.
- Auditing is very time consuming and resource-dependent but, according to our survey, not dependent on the size of the organization.
- The government auditors stressed the importance of having control over your systems; emphasis is on the integrity of the data and then on the confidentiality of the data. Covered Entities must have audit log reports that capture any inappropriate activity.
- Auditing might be virtually impossible with old legacy systems and, practically, some consideration must be given to the level of sophistication of the technology that may prevent auditing. But, a good faith effort must be made, given the limitations. For instance, you may have to prove, and document that the capability to audit does not exist. Use the standard of reasonableness.
- It is clear that creating or updating a Human Resources disciplinary policy to include disciplinary action for violating HIPAA Security policies is necessary to comply with this standard.
- The majority of respondents appear to have implemented a disciplinary policy to meet the requirement.

3.7.3 Conclusions/Recommendations

- Most information systems provide some level of audit controls with a reporting method, such as audit reports. These controls are useful for recording and examining information system activity, especially when determining if a security violation occurred.
- It is important to point out that the Security Rule does NOT identify data that must be gathered by the audit controls or how often the audit reports should be reviewed. A Covered Entity must consider its risk analysis and organizational factors, such as current technical infrastructure, hardware and software security capabilities, to determine reasonable and appropriate audit controls for information systems that contain or use EPHI.[2]

[2] DHHS HIPAA Security Series, #4 Security Standards: Technical Safeguards

- Covered Entities should consider
  - The audit control mechanisms that are reasonable and appropriate to implement so as to record and examine activity in information systems that contain or use ePHI

  - The audit control capabilities of information systems with ePHI

  - If the audit controls implemented allow the organization to adhere to policy and procedures developed to comply with the required implementation specification at § 164.308(a)(1)(ii)(D) for Information System Activity Review

- The HIPAA Security Rule also includes an implementation specification for **Information System Activity Review** that requires Covered Entities to routinely review records of information system activity such as audit logs and access reports, enabling Covered Entities to determine if any ePHI is used or disclosed in an inappropriate manner. These information system activity review procedures should be customized to meet each Covered Entity's risk management strategy and take into account the capabilities of all information systems with ePHI.

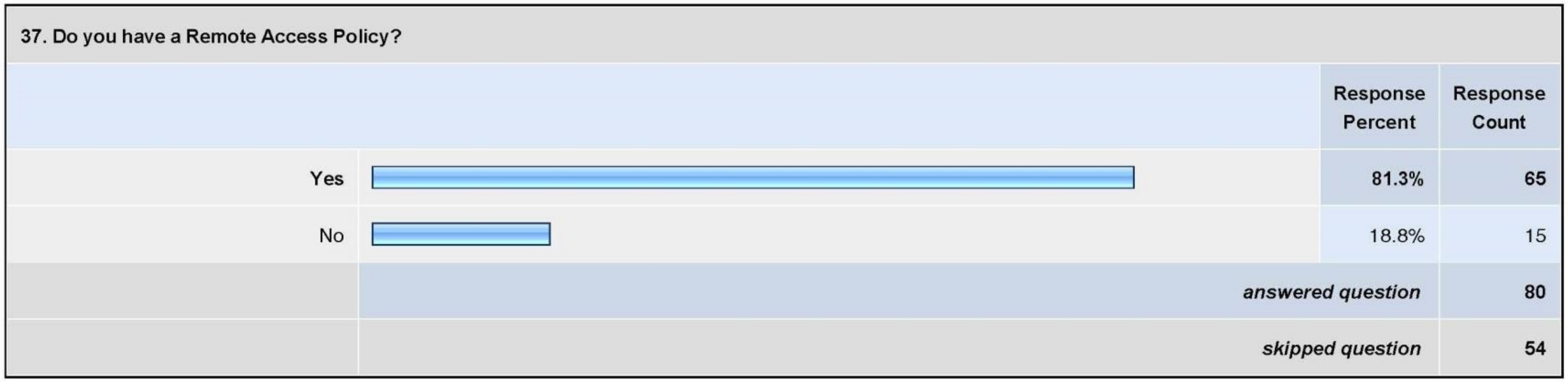
- Covered Entities should consider:
  - The audit and activity review functions of the current information systems

  - If the information systems functions are being used adequately and monitored to promote continual awareness of information system activity

  - Which logs or reports are generated by the information systems

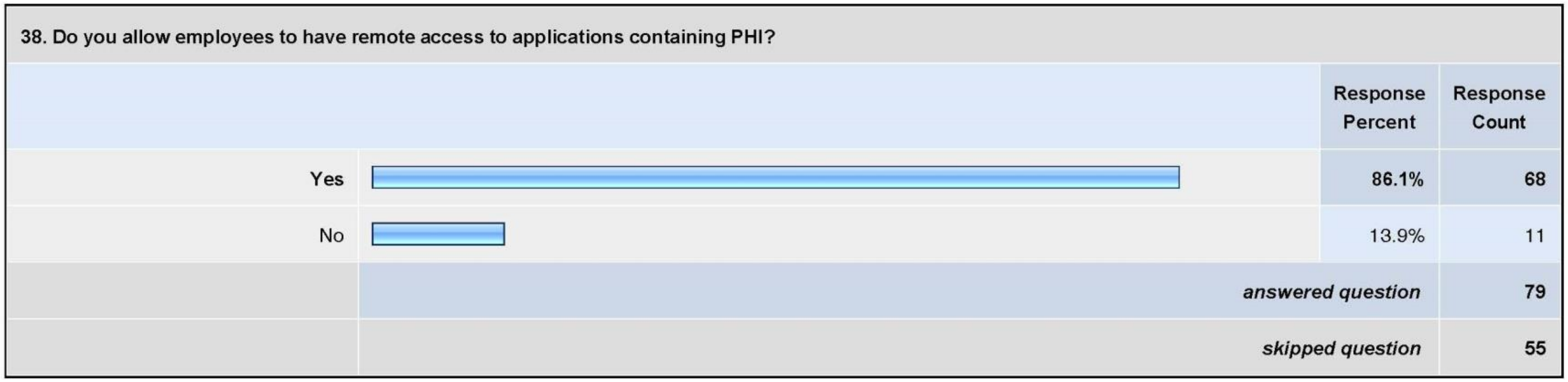
  - Developing of a policy that establishes which reviews will be conducted and a procedure that describes the specifics of the reviews

3.8 Remote Access



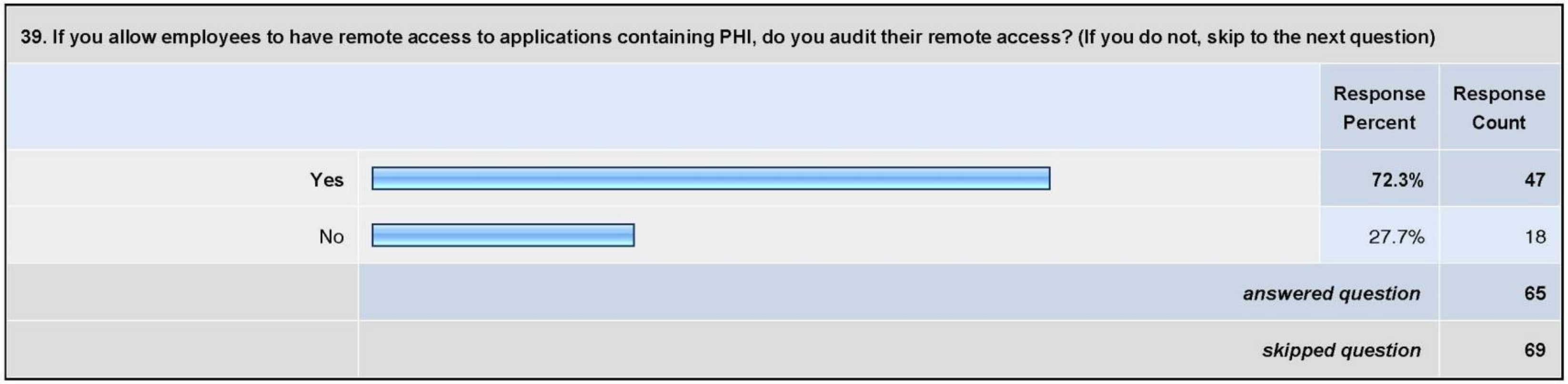
37. Do you have a Remote Access Policy?

	Response Percent	Response Count
Yes	81.3%	65
No	18.8%	15
answered question		80
skipped question		54



38. Do you allow employees to have remote access to applications containing PHI?

	Response Percent	Response Count
Yes	86.1%	68
No	13.9%	11
answered question		79
skipped question		55



39. If you allow employees to have remote access to applications containing PHI, do you audit their remote access? (If you do not, skip to the next question)

	Response Percent	Response Count
Yes	72.3%	47
No	27.7%	18
answered question		65
skipped question		69

3.8.1 Data/Results

- The majority, or 81.3%, of respondents confirm they have a Remote Access Policy
- The majority, or 86.1%, also state they allow employees with remote access to access applications containing PHI
- 72.3% state they audit the remote access of employees

3.8.2 Committee Observations

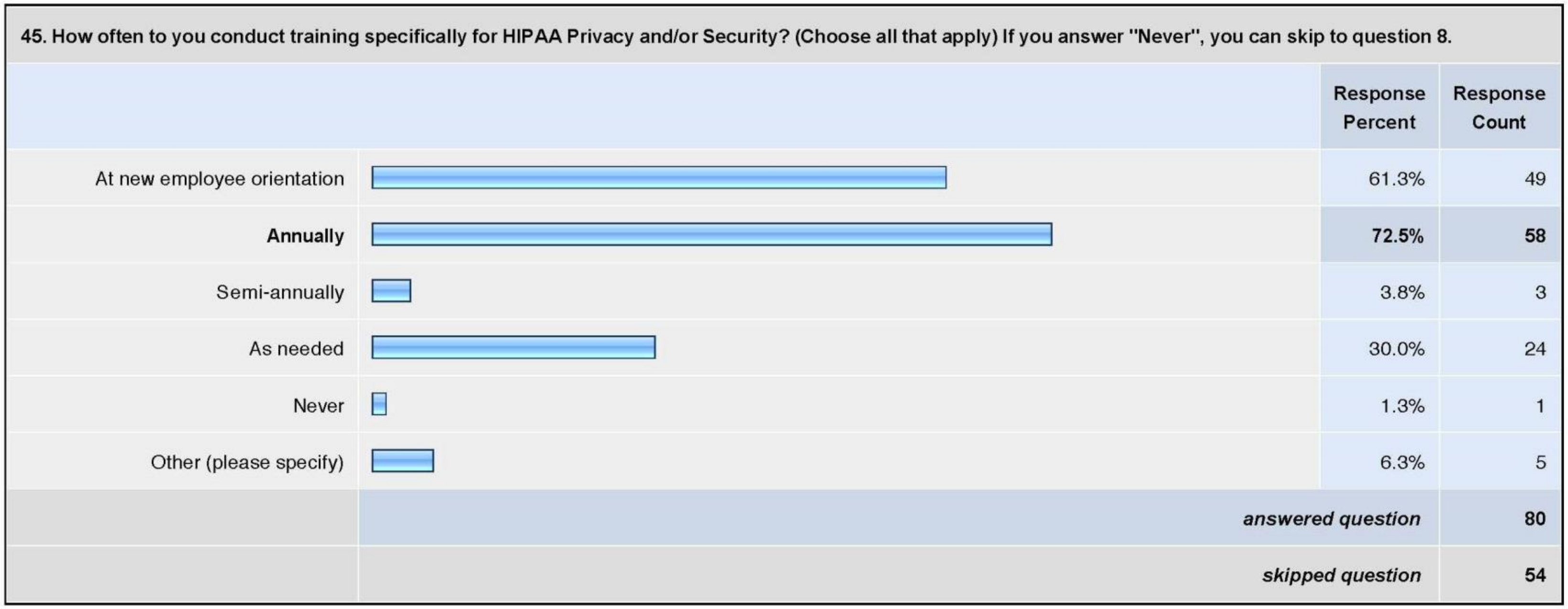
- Whether or not remote access is audited was not dependent on whether the organization was large or small.
- High speed remote access makes organizational networks a very lucrative target. Technology provides for feature-rich sets of capabilities and functions, but each organization must carefully pick through the functionalities to ensure the risk profile suits your needs, and the security needs of the information the networks hold. Here is list of technical considerations:
  - Is personally-owned equipment allowed?
  - Client-based, clientless VPN.
  - Level of encryption.
  - Allowing or disallowing “split-tunneling”
  - Network Access Control (NAC) requirements.
  - Authentication requirements – one-factor, two-factor
  - Logging and monitoring.
  - Idle-time outs.
  - Copying and printing of files at remote locations.
  - Access to systems and resources.
  - Contractor management.
  - Incident detection and reporting.
- Remote access to networks and resources increases your risk profile. Establishing remote access creates high-speed connections into homes and businesses of all sizes that are “always on/always available.” It is important to balance the perceived benefit to the organization before accepting the additional risk. At the same time, this technology has been around for years, and it would be a truly rare organization that does not already have remote access in place.
- If you allow remote access, how do you monitor or prevent printing of PHI? If you remove the driver on the terminal printer, users cannot print at home.
- Is limiting file transfers an option?

3.8.3 Conclusions/Recommendations

- Although 81.3% of respondents indicated they have a remote access policy in place, it is critical that the policy is up to date and revised at least annually to be sure it keeps pace with all the emerging technologies that require support. It has become an expectation that IT and security/compliance professionals can and will be able to provide access to mission critical applications and functions with risk profiles that are within acceptable and audit-permissible limits. It is now technically possible to log into and control servers from smart phone type devices. Convergence will increase demands on good and comprehensive policies.

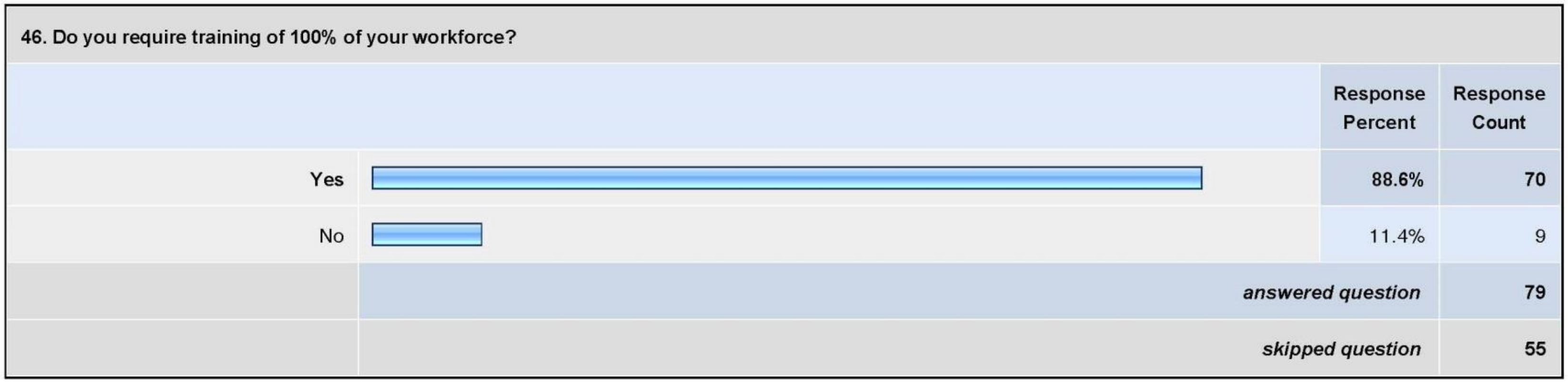
- The Remote Access Policy must be distributed and employees must be trained. Enforcement and sanction provisions are also key to a comprehensive security strategy.
- Prior to being granted remote access privileges, employees should be required sign an attestation indicating acknowledging and agreeing to abide by the standards and policies and procedures established by the organization to protect and secure PHI that is accessed remotely.
- In considering the management of remote access, there really are only 2 options: restrict the use of PCs not owned or under the control of the organization or run the risks inherent in the use of remote access and manage the risk through organizational policies, education and discipline, which would also require auditing/monitoring.
- The biggest decision an enterprise may make once remote access is granted is whether or not access will be allowed from equipment that is not owned and configured by that organization. How do you protect internal networks from non-enterprise owned PCs? Some organizations cannot afford a laptop for everyone who may be interested in working from home. Simply having an organization provide a device does not mitigate all risk. It may decrease the risk of a worm or virus from entering your networks, but potentially not all unauthorized access. For example, what would prevent someone from allowing a family member from accessing a corporate laptop when it is on the desk or coffee table at home?
- Additionally, consider remote support from a software, hardware or services vendor. Many organizations allow an extranet capability, whereby contractors or business partners are allowed access, and sometimes at DBA or Administrator levels of control.   It might be expected that these resources are sitting within a partner’s secure network, but there is no way of knowing that is true – that their security posture is at least as good as your own.   So, while you could have a secure link between your networks and the XYZ Software Company, the person logging into your networks could be at his or her home in front of the TV, or on a wireless connection or coming in through a public PC in a hotel’s Internet Café.
- Clearly, there are many factors that externalize risk exposure, so each organization must perform its own analysis to ensure that whatever is decided is based on business needs, and acceptable levels of risk.
- Do not overlook all forms of access. For example, some employees may be able to get by with just access to e-mail. A web-based e-mail solution can get them what they need without other remote access concerns. Beware, however, since an employee could email themselves a document with a file attachment and could access information from a remote location – even saving that file to another workstation.   Some applications could be accessed via a web interface through a proxy server. This could save the expense VPN concentrator or other type of access device and allow access to only certain functions. Considering business objectives, consideration might be given to alternate technologies such as remote presentation technologies or virtual workstations

3.9 Training



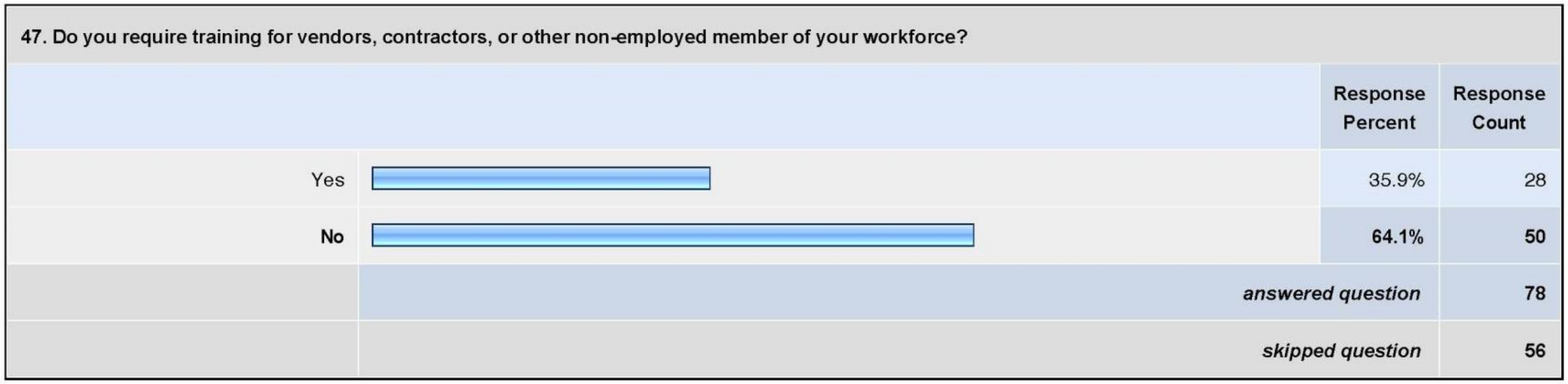
45. How often to you conduct training specifically for HIPAA Privacy and/or Security? (Choose all that apply) If you answer "Never", you can skip to question 8.

	Response Percent	Response Count
At new employee orientation	61.3%	49
Annually	**72.5%**	**58**
Semi-annually	3.8%	3
As needed	30.0%	24
Never	1.3%	1
Other (please specify)	6.3%	5
	answered question	**80**
	skipped question	**54**



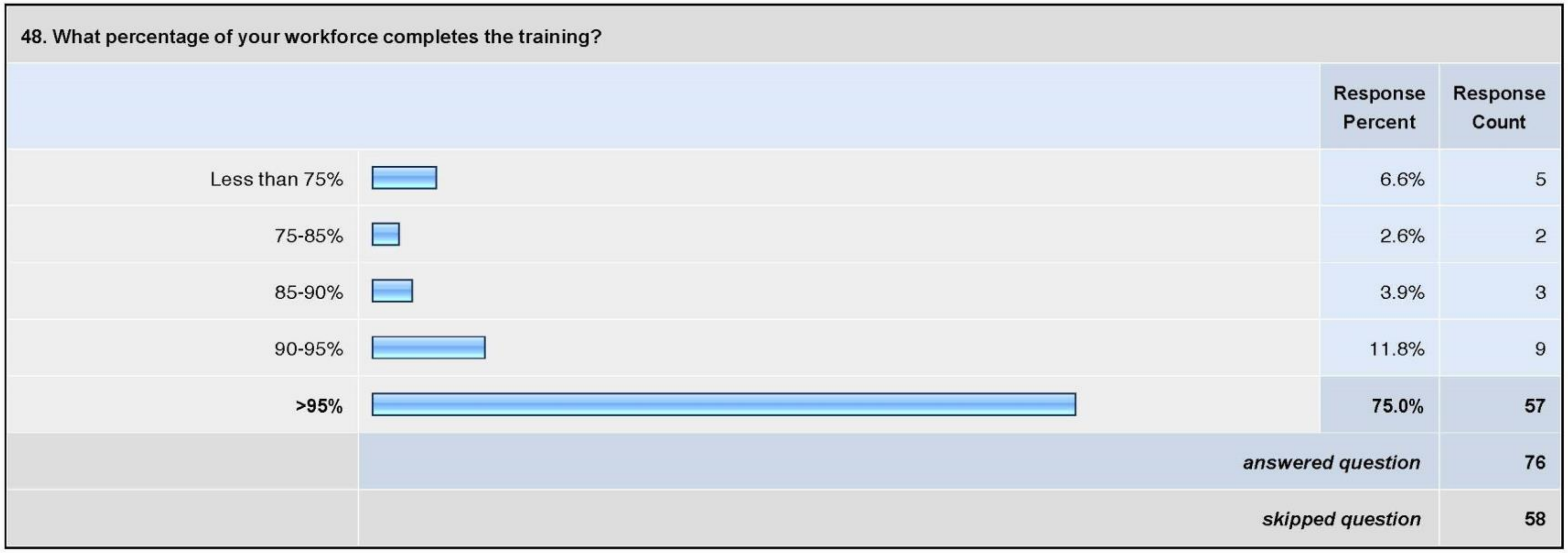
46. Do you require training of 100% of your workforce?

	Response Percent	Response Count
Yes	**88.6%**	**70**
No	11.4%	9
	answered question	**79**
	skipped question	**55**



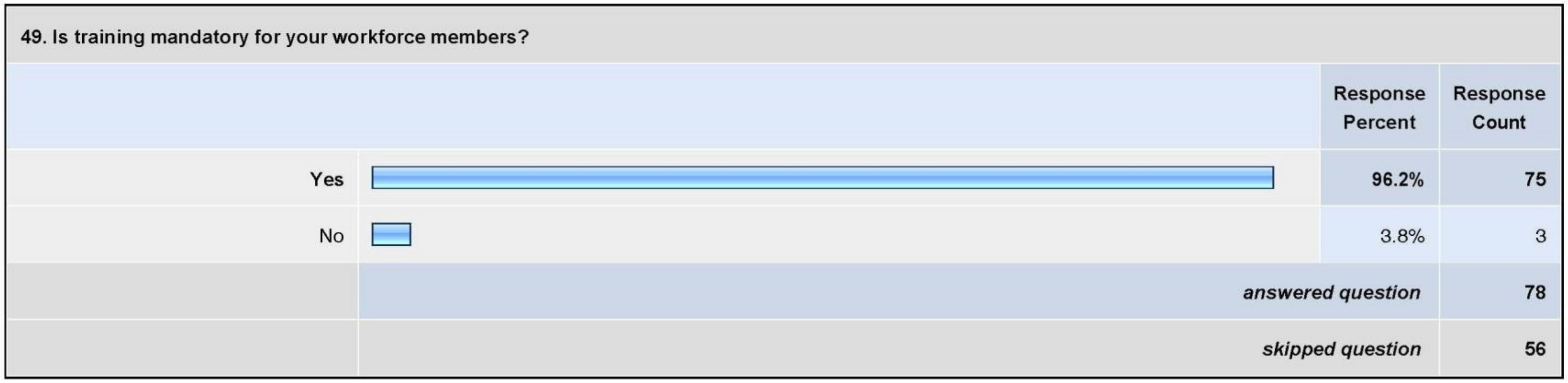
47. Do you require training for vendors, contractors, or other non-employed member of your workforce?

	Response Percent	Response Count
Yes	35.9%	28
No	**64.1%**	**50**
	answered question	**78**
	skipped question	**56**



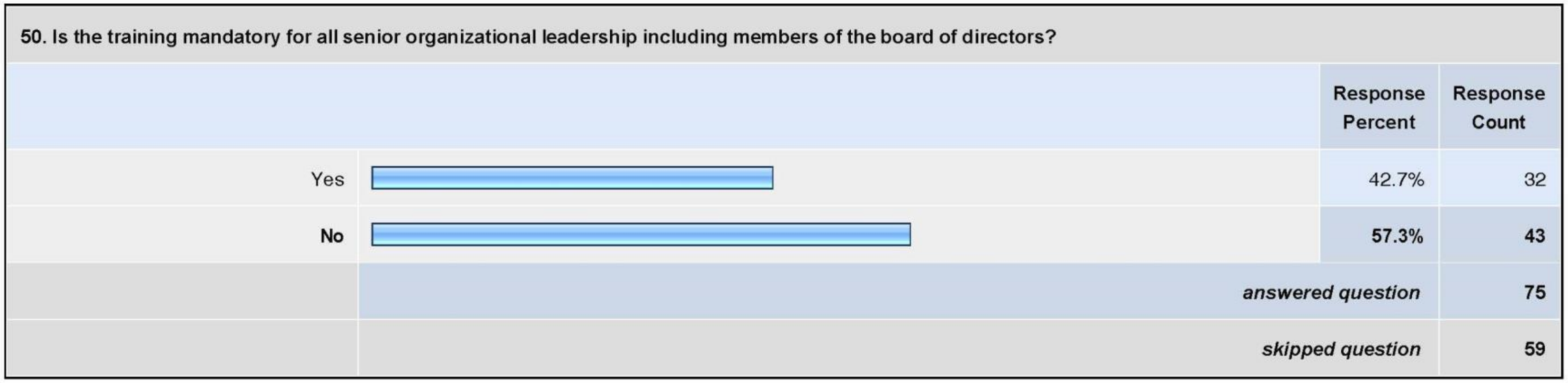
48. What percentage of your workforce completes the training?

	Response Percent	Response Count
Less than 75%	6.6%	5
75-85%	2.6%	2
85-90%	3.9%	3
90-95%	11.8%	9
>95%	**75.0%**	**57**
	answered question	**76**
	skipped question	**58**



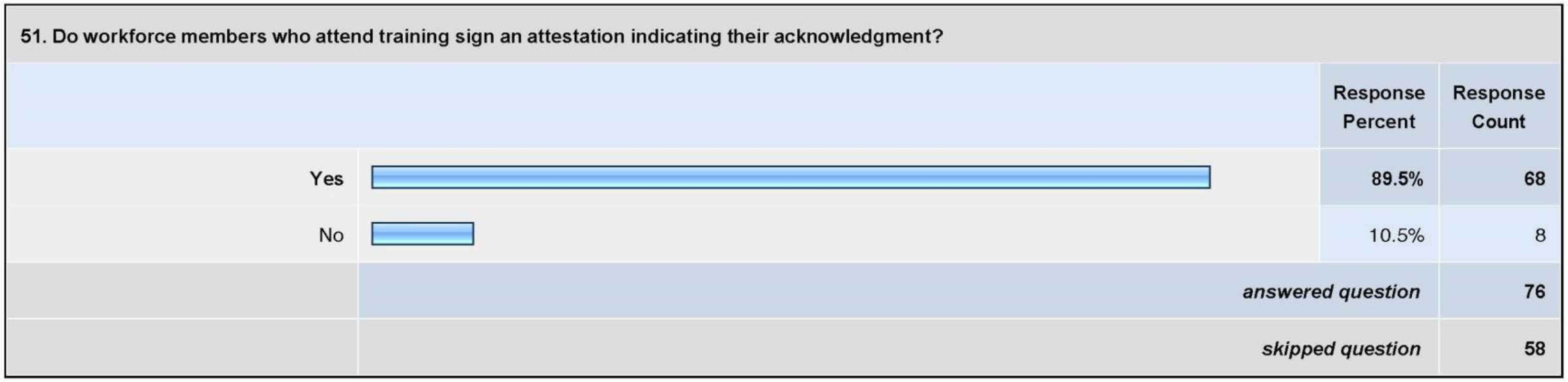
49. Is training mandatory for your workforce members?

	Response Percent	Response Count
Yes	96.2%	75
No	3.8%	3
answered question		78
skipped question		56



50. Is the training mandatory for all senior organizational leadership including members of the board of directors?

	Response Percent	Response Count
Yes	42.7%	32
No	57.3%	43
answered question		75
skipped question		59



51. Do workforce members who attend training sign an attestation indicating their acknowledgment?

	Response Percent	Response Count
Yes	89.5%	68
No	10.5%	8
answered question		76
skipped question		58

3.9.1 Data/Results

- When asked how often training specific to HIPAA Privacy/Security is conducted, the responses were:
  - 72.5% hold training annually
  - 61.3% conduct this training at new employee orientation
  - 30% indicate they only conduct training as needed
  - 3.8% hold training semi-annually
  - 1.3% indicate they do not conduct training
  - 6.3% answered other –check narrative comments
- 88.6% responded that they train 100% of their workforce; 11.4% indicate they do not train 100% of their workforce
- 35.9% train vendors, contractors, or other non-employed members of their workforce; 64.1% do not train these members of their workforce
- 96.2% state that training is mandatory for workforce members but only 57.3% state training is mandatory for all senior organizational leadership including members of the BOD; 42.7 % indicate training is mandatory for senior leadership
- 75% of respondents indicated that 95% of their workforce completes training
- 89.5% of organizations require workforce members to sign an attestation indicating their acknowledgment of HIPAA training; only 10.5% do not require this attestation

3.9.2 Committee Observations

- The results of the survey clearly indicate that the majority of respondents conduct training annually. Training is the key to compliance by creating awareness. However, 11.4% indicate they do not train 100% of their workforce.
- It is difficult to understand why the majority of respondents do not make training mandatory for their senior leadership. Senior leadership needs to understand the importance of HIPAA Security and, now, breach reporting obligations. Also, even though the Board of Directors may not have access to PHI they still need to understand the standards in the organization. This will require a different level of training than the majority of the workforce.

3.9.3 Conclusions/Recommendations

- HIPAA Privacy/Security training should be conducted and documented at new employee orientation.
- To protect the organization all workforce members should be required to sign an attestation indicating their acknowledgement of HIPAA Privacy/Security training.
- All Covered Entities should have conducted and documented mandatory HIPAA Privacy/Security training for all workforce members. In addition, periodic retraining should be given whenever environmental or operational changes affect the security

of PHI. Changes may include: new or updated policies and procedures; new or upgraded software or hardware; new security technology; or even changes in the Security Rule.[3]

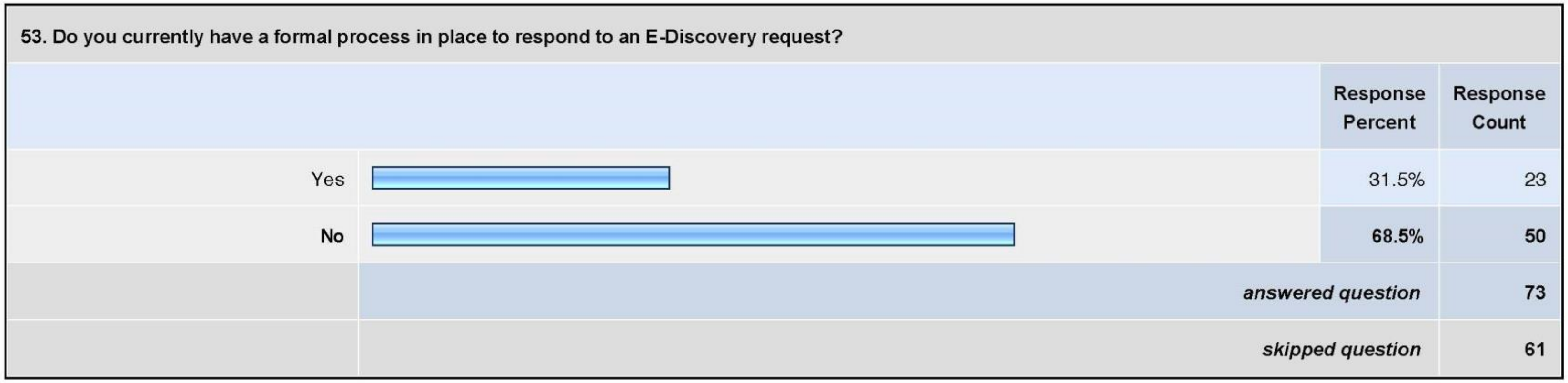
- In terms of how often to repeat the HIPAA Privacy/Security training to all workforce members the regulations do not require annually; however, to provide consistent awareness Security Networking Group's recommendation is to conduct training annually.
- The HIPAA Privacy regulations at section 164.530(b)(1) indicate as a standard that a covered entity must train <u>all members</u> of its workforce on the policies and procedures with respect to protected health information <u>as necessary and appropriate</u> for the members of the workforce to carry out their functions within the covered entity. The implementation specifications indicate that a covered entity must provide and document the training that meets the standard as follows:

    - To each member of the Covered Entity's workforce by no later than the compliance date for the covered entity;
    - Thereafter, to each new member of the workforce within a reasonable period of time after the person joins the Covered Entity's workforce; and
    - To each member of the Covered Entity's workforce whose functions are affected by a material change in the required policies or procedures within a reasonable period of time after the material change becomes effective.

- The HIPAA Security regulations require that a security awareness and training program should be implemented for <u>all members</u> of its workforce (including management).
- The addressable implementation specifications indicate that to meet the standard a Covered Entity should train on/with:
    - *Security reminders*. Periodic security updates.
    - *Protection from malicious software.* Procedures for guarding against, detecting, and reporting malicious software.
    - *Log-in monitoring*. Procedures for monitoring log-in attempts and reporting discrepancies.
    - *Password management*. Procedures for creating, changing, and safeguarding passwords.

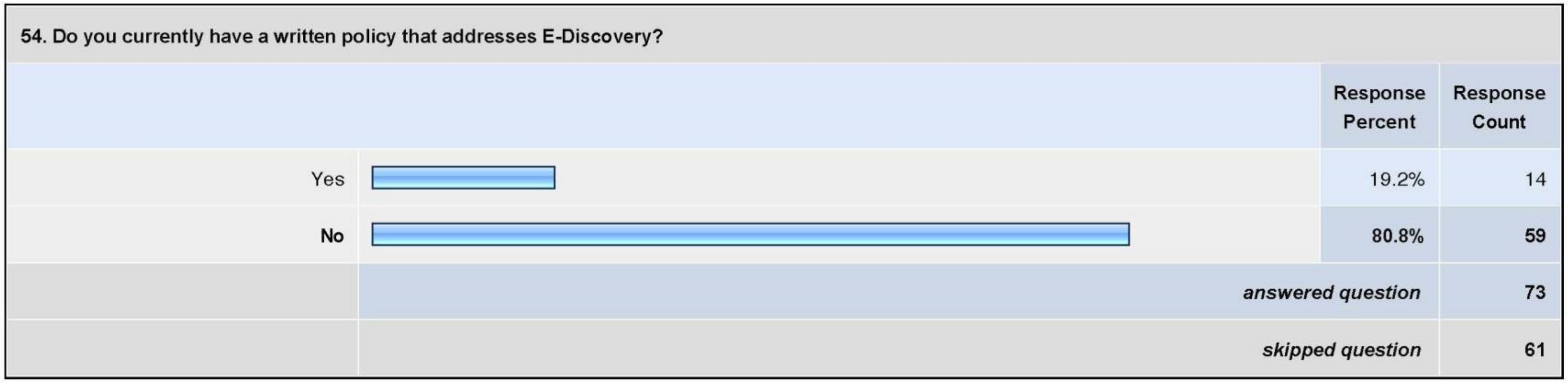
[3] DHHS HIPAA Security Series, #2 Security Standards: Administrative Safeguards

3.10 E-Discovery



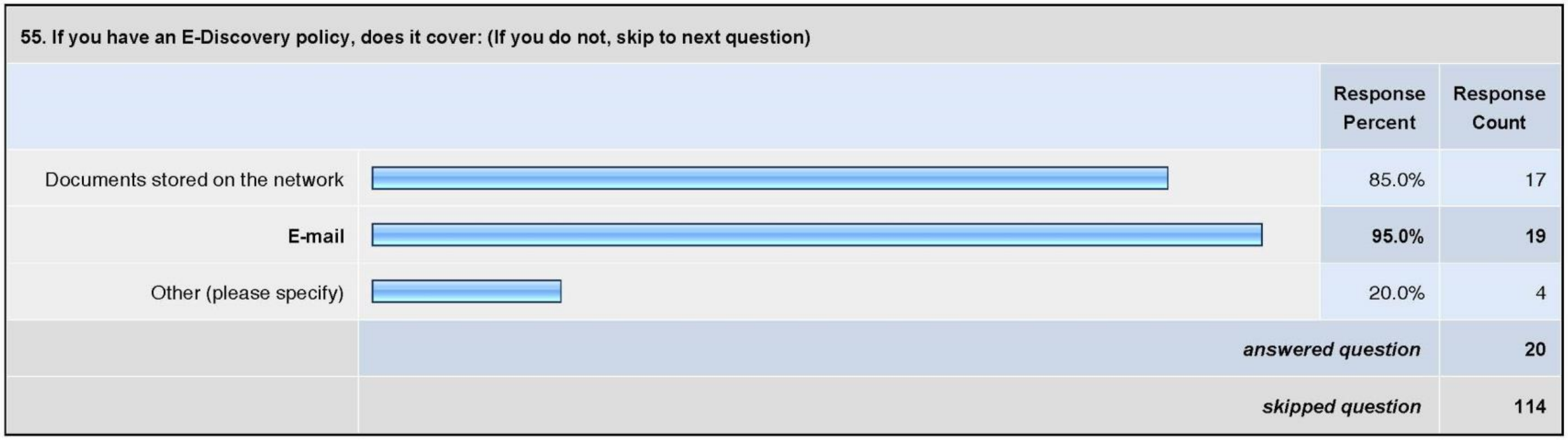
53. Do you currently have a formal process in place to respond to an E-Discovery request?

		Response Percent	Response Count
Yes		31.5%	23
No		**68.5%**	**50**
		answered question	**73**
		skipped question	**61**



54. Do you currently have a written policy that addresses E-Discovery?

		Response Percent	Response Count
Yes		19.2%	14
No		**80.8%**	**59**
		answered question	**73**
		skipped question	**61**



55. If you have an E-Discovery policy, does it cover: (If you do not, skip to next question)

	Response Percent	Response Count
Documents stored on the network	85.0%	17
E-mail	**95.0%**	**19**
Other (please specify)	20.0%	4
answered question		**20**
skipped question		**114**

3.10.1 Data/Results

- Approximately 1/3, or 31.5%, state they have a formal process in place to respond to an E-Discovery request; 68.5% indicate they do not have a process for responding to an E-Discovery request
- Only 19.2% respond that they have a written policy that addresses E-Discovery; 80.8% do not have a written policy
- For those who have a written E-Discovery policy:
  - 85% indicate the policy covers documents stored on the network
  - 95% indicate the policy covers e-mail
  - 20% indicate the policy covers other types of data

3.10.2 Committee Observations

- Serious consideration must be given to the legal ramifications of E-Discovery. While an e-mail retention policy is a good start, as indicated above, E-Discovery is not limited to just e-mail. Any and all documents stored electronically are subject to the E-Discovery rules.
- Moreover, the length of retention is almost as important as the documented policy itself. The longer electronic documents are saved, the longer the period of time an opposing party can look back into the electronic records.
- With exponential growth in electronically stored information has come expanding demands for disclosure of electronic information in litigation. Many cases are now litigated with each side primarily disclosing only electronically stored documents, including contracts, spreadsheets, policies, and correspondence. First formally recognized in the Federal Rules of Civil Procedure ("FRCP") in December 2006, the issue of how electronic information can be accessed for purposes of litigation has become known as "e-Discovery". Under the FRCP, parties can be penalized for inappropriate destruction of electronic documents, and the FRCP further require parties to disclose electronic documents stored in the "usual course of business",

unless such documents were lost as a result of “routine, good faith operation of an electronic information system.” The practical result of these rules on day-to-day operations for businesses can be summarized as follows – appropriate policy development, including a record retention schedule and litigation hold policy, are a minimal necessity for good business planning.

- The survey revealed that the length of retention varied greatly from entity to entity, from two weeks to “forever”. Good practice regarding retention policies drives the retention period by the data type, not by the data medium. Currently, just more than half of respondents, 54.3%, store all e-mail regardless of content. This emphasizes the importance of education and enforcement of your policy.

3.10.3 Conclusions/Recommendations

- Know who leads this effort in your organization.
- Education and enforcement of the policy are as critical to properly controlling E-Discovery risk as is policy development.