Communications of the IIMA

Volume 4 | Issue 2 Article 7

2004

Policies, Procedures, and Devices Used by U.S. Hospitals for HiPAA Privacy and Security Compliance

Diane C. Davis
Southern Illinois University

Jeff Squibb
Southern Illinois University

Recommended Citation

Davis, Diane C. and Squibb, Jeff (2004) "Policies, Procedures, and Devices Used by U.S. Hospitals for HiPAA Privacy and Security Compliance," *Communications of the IIMA*: Vol. 4: Iss. 2, Article 7.
Available at: http://scholarworks.lib.csusb.edu/ciima/vol4/iss2/7

Policies, Procedures, and Devices Used by U.S. Hospitals for HIPAA Privacy and Security Compliance

Diane C. Davis

Information Management Systems Department, MC 6614, Southern Illinois University, Carbondale, IL 62901
(618) 453-7296; Fax: (618) 453-7254; dcdavis@siu.edu

Jeff Squibb

Information Management Systems Department, MC 6614, Southern Illinois University, Carbondale, IL 62901
(618) 453-8876; FAX: (618) 453-7254; jsquibb@siu.edu

ABSTRACT

The purpose of the study was to identify the policies and procedures required in U.S. hospitals to meet the requirements of the Health Information Portability and Accountability Act (HIPAA). A major aspect of the study focused on the degree of change required to meet the security standards and on the types of security devices used by the hospitals. Findings from a survey of 286 U.S. hospitals found the greatest amount of change needed to meet HIPAA security compliance were changes resulting in increased Information Systems (IS) budget requirements, changes to network monitoring, and additional hiring in the IS department.

INTRODUCTION AND REQUIREMENTS OF HIPAA

Americans are privileged to have the freedom to make choices regarding many day-to-day activities as well as choices regarding major life decisions including choice of healthcare provider. Many factors are considered in relation to healthcare choices. Individuals want to select someone in the medical profession who can be trusted for medical treatment and handling of personal medical health information. It is expected that confidentiality will be maintained and that the trust relationship between patient and provider not be compromised. Todd Fitzgerald, co-chair of the Security Taskforce for HIPAA (2004), emphasizes the distinction of privacy and security as follows:

> Privacy issues address the rights of the individual with respect to this trust relationship, whereas security is the mechanism that ensures that this privacy is reasonably maintained throughout the system. True privacy of information cannot be achieved without adequate security controls (p. 1920).

The establishment and delivery of the rules and regulations of HIPAA have been a long time coming. The HIPAA statute was enacted to protect employees when they changed jobs so they would not lose health insurance benefits; this is the idea of portability of their insurance meaning it could be moved from one company to another. The new employer could not exclude the employee from their group plan because of pre-existing conditions as long as the employee maintained COBRA coverage for the time period between jobs (Smith, 2003). In order to address additional risks, the administrative simplification subtitle was added to HIPAA to standardize the method for transmitting health information electronically. Then due to increased use of electronic commerce and related technologies, more concerns were created about privacy and security of patient information.

The compliance date for the Privacy Rule was set for April 14, 2003 and the compliance date for the Security Rule was set for April 21, 2005 (Fitzgerald, 2003, p. 50). Small health plans have to be compliant within the year following those dates. The main purpose of HIPAA security is to provide assurance that covered entities can guarantee the privacy rights of their patients and health plan members. Many healthcare entities are changing network infrastructure, policies, procedures, software, and hardware to meet compliance for the Security Rule.

The Security Rule contains security standards designed to define the safeguards needed to protect the confidentiality, integrity, and availability of electronic protected health information (Fitzgerald, 2004). Therefore, it is necessary for healthcare entities covered under the Act to meet the security standards; however, some are called "required implementation specifications" and some are "addressable implementation specifications." In other words, some standards are required of all entities and other are to be addressed according to the needs of the organization in relation to size, complexity of systems, capabilities, cost of security measures, and potential risks to the electronic information. "The three safeguard categories of Administrative, Physical, and Technical contain a total of 18 security standards that must be addressed" (Fitzgerald, 2003). These are summarized in the table below (Fitzgerald, 2003, 2004):

Security Standards		
Administrative Safeguards	**Physical Safeguards**	**Technical Safeguards**
Security Management Process	Facility Access Controls	Access Control
Assigned Security Responsibility	Workstation Use	Audit Controls
Work force Security	Workstation Security	Integrity
Information Access Management	Device and Media Controls	Person or Entity Authentication
Security Awareness and Training		Transmission Security
Security Incident Procedures		
Contingency Plan		
Evaluation		
Business Associate Contracts		

Table 1: Security Standards

Some of the security standards are comprised of multiple required implementation specifications. For example, the security management process (as shown in Table 1 as the first Administrative safeguard) has four required implementation specifications. These are (1) risk analysis, (2) risk management, (3) sanction policy, and (4) information system activity review (Fitzgerald, 2003; Smith, 2003).

The Healthcare Information and Management Systems Society (HIMSS) is a membership organization focused exclusively on providing leadership for optimal use of healthcare information technology and management systems for improving human health (HIMSS, 2004). HIMSS and Phoenix Health Systems conduct quarterly surveys to identify the status of the healthcare industry regarding implementation of the Privacy Rule (April 2003), Transactions and Code Sets compliance (October 2003), and the Security Rule (April, 2005). Even though the HIPAA Transactions and Code Sets and Privacy Rules have passed the deadlines for compliance, not all providers, payers, clearinghouses and vendors indicate they are ready to conduct all HIPAA standard transactions or are totally compliant with the Privacy Rule. According to Phoenix Health Systems' Winter 2004 Survey of 631 healthcare industry representatives, 20% of the providers and 14% of the payers reported that they remain non-compliant with the Privacy rule, even nine months after its effective deadline of April 14, 2003 (Phoenix Health Systems, 2004).

The American Health Information Management Association (AHIMA) also conducted research to assess the current state of HPAA privacy within the healthcare industry. Their study which included privacy officers, those functioning as privacy or security officers without the formal titles, and other HIPAA team participants in the process of achieving compliance, released their results the second week of April, 2004. Out of the 1,192 survey respondents, 58 percent had designated privacy or security officials, 11% said they were functioning as privacy or security officials without the formal titles, and 31% stated they served on the HIPAA privacy and security teams or committees. The majority of the respondents (68%) reported at least 85% compliance with the Privacy Rule. In regard to changes in their health and information systems, they found that more than half of the respondents (55%) required some kind of upgrade to electronic software or application systems to reach HIPAA privacy implementation. More specifically, 44% of the respondents said the purchase or development of new software was required (AHIMS, 2004).

The impact of the Health Insurance Portability and Accountability Act (HIPAA) has been tremendous in all health related entities as well as to those in the information systems field. There has been a greater need by healthcare entities to evaluate existing security mechanisms and to implement new systems (everything from physical devices such as IDs and smart cards to firewalls and biometric systems). This Act is not the only legislation that has been passed in the last few years that has required organizations to undergo a great deal of change to provide privacy and security of electronic information. The Gramm-Leach-Bliley Act (GLBA) and the Sarbanes Oxley Act (SOXA) are just a couple of the others that have requirements that companies must meet, and it is important that they do so and on a timely basis to mitigate any liabilities that could result from lack of compliance. The first step in this process is to make sure the organization has a security policy/plan to follow (Peled and Troyansky, 2004).

RATIONALE OF THE STUDY

The researchers of this study focused primarily on the HIPAA Security Rule specifically the degree of change required to various policies and procedures within hospitals toward meeting the 18 security standards and on the types of security devices (hardware and software) used by the hospitals.

As healthcare entities progress toward compliance, it is helpful to identify roadblocks and share with other entities some of the ideas and solutions for achievement. Also, it is essential for students in the healthcare and information technology fields to learn about the HIPAA issues hospitals are facing and how they are accomplishing compliance. Many of today's students will soon be employed in the field to assist in this endeavor as well as to maintain many of the policies and procedures now being implemented. Therefore, the researchers felt the need to identify (1) the activities and procedures taking place in U. S. hospitals in regard to reaching HIPAA compliance, (2) the amount of change required in information systems technologies and procedures to reach compliance for the security standards, and (3) the security devices and methods employed by the hospitals to ensure the privacy and security of electronic health information.

METHODOLOGY

After a thorough review of the literature and study of the HIPAA regulations, a survey was written by the researchers during the summer of 2003 to examine the privacy and security policies used by hospitals in the United States. There were four main parts to the survey: (1) the demographic characteristics of the respondents, such as title and experience, and the size and type of hospitals; (2) the facility's strategies for achieving HIPAA compliance, (3) the perceptions of the respondents (HIPAA officers) regarding their level of compliance with the security specifications that were categorized under the 18 security standards and their perceptions of the degree of change taking place at the hospital due to the HIPAA requirements; and (4) the security devices used by the hospitals to meet the requirements.

Although some questions were very similar to the ones used by HIMSS/Phoenix Health Systems survey and the AHIMA survey, such as identifying major roadblocks to reaching compliance and degree of compliance achieved, this survey focused more on levels of compliance related to specific security standards and on the level of change the respondents perceived within their facility based on HIPAA regulations.

The survey instrument was reviewed early in the fall by a panel of experts which included medical personnel and information security personnel in local hospitals. Revisions were made to the survey instrument based on the comments of the reviewers. The survey was then approved by the Human Subjects Committee at the university employing the researchers before it was pilot tested. With that approval, the survey was sent to ten randomly selected hospitals from a national list of hospitals. It was also reviewed by three attendees at the E-Security conference held in St. Louis, Missouri, in October 2004. Comments from these experts were reviewed and used as feedback for final revision of the instrument.

A database of 1000 randomly selected member hospitals of the American Medical Association was purchased from Third Wave Research. A mailing including a cover letter, survey instrument, and self-addressed return envelope was prepared and ready the end of November; however, the researchers decided to wait to send the mailing until after the holidays. Therefore, the mailing went out the last week of the year and surveys were received by hospital staff the first week of January 2004. A follow-up mailing was sent the second week of February. A total of 286 surveys were returned for a response rate of 28.6%. The responses were transferred to scantron sheets, a program was written, and the data were tabulated using SAS Version 8.

FINDINGS OF STUDY

The findings summarized below are based on the responses from the 286 surveys that were returned. Some respondents did not answer all questions, so the total number of respondents for each question varied slightly. Also, several questions asked the respondents to provide more than one answer so the total percent does not equal to 100% in many cases.

Size of Hospitals

In regard to the size of the hospitals surveyed, they were asked how many beds they had at their facility. They were also asked if they were a part of an integrated hospital network system; and if so, what was the total number of beds at all locations. A large majority of hospitals (83%) indicated that they had less than 250 beds at their facility; 13% indicated they had 250 to 499 beds; and 4% had 500 or more beds at the facility. One hundred eight of the hospitals (41%) were a part of an integrated hospital network. Of these 108 hospitals (out of the total 286) that were integrated, 26% indicated the total number of beds at all locations was 2000 or greater; 25% said they had 1000-1999 at all locations; 16% had 500 to 999 beds; 15% had 250 to 499 beds; and 19% had less than 250 beds at all locations.

Job Titles and Job Needs

When the respondents were asked which of the provided titles best matched their job description, the largest number of respondents indicated a title of privacy officer. Forty-six percent indicated that privacy officer matched their job title and 32% indicated HIPAA officer. When the question was written it was intended that the respondents would mark only one answer; however, a few respondents marked more than one, so all answers were coded and are shown in Table 2.

Title	Number	Percent
HIPAA Officer	91	31.82
Privacy Officer	132	46.15
Security Officer	19	6.64
Compliance Officer	52	18.18
Health Information Manager	29	10.14
Other	41	14.34

Table 2: Job Titles

The respondents were also asked what new job titles had been created at their facility to meet HIPAA compliance. This time they were asked to mark all that applied. The results can be seen in the Table 3.

Title	Number	Percent
HIPAA officer	100	34.97
Privacy officer	223	77.97
Security officer	159	55.59
Other	21	7.34
None of the above	16	5.59

Table 3: New Job Titles Created to Meet HIPAA Compliance

A large majority of the respondents (89%) indicated that no new person outside the system was hired for any of the above listed job titles. Of the 11% that did hire an outside person, the largest number indicated the new position was for a privacy officer. Those who indicated that the HIPAA officer duties were added to a currently existing position said they came primarily from the medical records/health information department or division.

When asked what areas of responsibility the HIPAA officer engaged in on a recurrent basis, the majority of the respondents said privacy issues, training, compliance administration, and security issues. The findings can be seen in Table 4.

Area of Responsibility	Number	Percent
Privacy issues	266	93.01
Security issues	157	54.90
Training	227	79.37
Compliance administration	178	62.24
Transaction code sets	87	30.42
Other (non-HIPAA) tasks	92	32.17

Table 4: Areas of Responsibility of HIPAA Officers

Although the majority of the respondents (66%) indicated that they spent 25% or less of their time on HIPAA related duties, it is interesting to note that 26% spent 26% to 50% of their time on these duties, 4% spent 51% to 75% of their time, and another 4% spent 76% to 100% of their time working with HIPAA requirements.

Security Issues

When asked about the physical on-site methods the facility used to provide HIPAA security compliance, the majority of respondents (58%) indicated they used electronic authorization for entry into secure areas (such as swipe cards or access codes), the next largest was a security guard or other security personnel (41%). Only 5% indicated they used a service provider for physical on-site methods.

Forty-six percent of the respondents also indicated that they did not have an Incident Response Team. Of those that did have an Incident Response Team, the privacy officer and/or HIPAA officer were the ones held responsible for these issues.

When the respondents were asked how near they were to HIPAA security compliance (April 2005 deadline), almost half estimated less than 50% compliant. The findings can be seen in Table 5.

Percent of Compliance	Number	Percent
0-25%	44	15.44
26-50%	89	31.23
51-75%	80	28.07
76-100%	72	25.26

Table 5: How Near Hospital was to HIPAA Security Compliance

Over one-third of the respondents (35%) indicated they were using outside consultants for one of the three main aspects of HIPAA (privacy, transactions, and security). Of those, 21% said they had consultants for security, 19% for privacy, and 19% for transactions. Many of these were using consultants for two or more of these three areas.

The greatest reported roadblock toward reaching security compliance was not enough financial resources (22%). Other roadblocks were interpretation of HIPAA regulations (17%), not enough work force (15%), and not enough time (10%). Once again several (12%) marked more than one "greatest" roadblock.

Therefore, the findings show that as a result of this legislative Act, many changes have been made to job positions within the hospital, specifically in regard to information systems. These changes include the creation of new job titles (for security officer), requirement of new responsibilities (for those in information systems) regarding policies and procedures established for HIPAA, and the use of more outside consultants in the areas of privacy and security.

Changes Required to Meet HIPAA Security Compliance

The respondents were given 11 items to evaluate in regard to their perception of the level of compliance with the HIPAA Security Rule they felt their facility had attained up to the time the survey was completed (January/February 2004). These were statements listing items from the 18 security standards (shown in Table 1); some of the items were listed separately and others were grouped together. They were asked to rate each on a scale of one to five, with five being the highest rating in attainment of compliance for that item. Means were calculated for all respondents' ratings, and the two items that were rated closest to compliance were (1) establishing policies/procedures for obtaining required business associate agreements and (2) policies/procedures for establishing physical safeguards to limit access to electronic information systems with facility access controls, workstation use and security, and device and media controls. The two areas in which they felt they were not as compliant were (1) policies/procedures for addressing security incidents (a response and reporting plan) and (2) policies/procedures for performing a periodic technical and non-technical evaluation of security practices governed by the Security Rule.

The respondents were given another list of items with a variety of types of changes that might need to occur to meet the 18 security standards. They were asked to evaluate each item in regard to their perception of the level of change that was needed at their facility (from the beginning to final deadline) to meet HIPAA security compliance. Once again, they rated each on a scale of one to five, with five being more change. The top four areas with the greatest amount of change needed as perceived by the respondents were (1) changes to the budget in information systems and (2) changes to network monitoring, (3) additional hiring in the information systems (IS) department and (4) changes to networking infrastructure and technologies. Table 6 shows all areas and the perceived amount of change required for each.

Area of Change	Mean Perception (1=Low, 5 = High)
Changes resulting in increased IS budget requirements	3.47
Changes to network monitoring	3.04
Additional hiring in the IS department	2.97
Changes to networking infrastructure and technologies	2.93
Changes to network security (such as firewalls or intrusion detection systems)	2.81
Greater use of an outside IS vendor or consultant	2.79
Closer working relationship between the Information Systems and Medical Records departments	2.79
Changes to policies regarding employee access to the Internet	2.73
Changes to institute tracking and access to medical records	2.71
Changes to physical access to servers, network devices, and workstations	2.70
Additional hiring in the Medical Records department.	2.57

Table 6: Changes Needed to Meet Compliance for Security Standards

The largest number of respondents indicated that firewalls and virtual private networks (VPNs) were their two main types of security devices/systems used within their facility. Seventy-three percent of the respondents indicated they used firewalls and 44% used VPNs to connect remote facilities or users. When asked what percentage of client workstations at their facility had antivirus programs, the largest number (90%) said 81 to 100% of the workstations. The largest number of respondents (48%) indicated that none or less than 20% of the workstations had personal firewall programs. The largest number of respondents (59%) also indicated they had none or less than 20% of their workstations using some type of encryption.

SUMMARY AND DISCUSSION

The researchers found that hospitals vary in the titles they assign to those responsible for HIPAA compliance. The largest number (46%) had the title privacy officer (this includes some that indicated they had a combination of titles). The next largest (32%) was HIPAA officer. There was indication that slightly over half of these individuals had existing positions in the medical records or health information areas and took on additional duties to meet HIPAA compliance requirements. Only 11% of the facilities hired a new person rather than assign the responsibilities to another existing employee. The researchers in this study found that 47% of the respondents estimated their facility to be at 50% or less toward reaching security compliance (at the time of the survey).

Most of the studies done by the health organizations (HIMSS, Phoenix Health Systems, and AHIMA) found that there are still many health entities that have not even reached complete privacy compliance even though the compliance date was April 14, 2003. Therefore, it will most likely be well after the assigned date of April 21, 2005 (or 2006 for small plans) before some entities reach complete compliance for the Security Rule. In this study, the largest number of respondents (31%) indicated they felt they were 26% to 50% compliant at this time for the Security Rule. This indicates many changes still need to be made to make sure the information on patients is kept secure so that only those who are supposed to have access can obtain the medical information desired. According to Phoenix Health Systems (2004), "With Security Rule compliance not required until April 2005, remediation efforts continue to progress slowly across the industry." Since hospitals will continue to deal with the need to meet compliance for years to come, current students in information systems and information management must understand the requirements, needs, solutions, and policies implemented. Some students of today will be those hospital HIPAA security officers and security consultants of the future. Educators and those in business and industry must work together to educate present and future employees with the ability to develop more efficient and effective methods, procedures, and technologies to meet the needs of the work place.

The respondents in this study indicated the following as major roadblocks: not enough financial resources (22%), interpretation of HIPAA regulations (17%), not enough work force (15%), and not enough time (10%). When the respondents of the HIMSS/Phoenix Health Systems' survey were asked the major roadblock to overall HIPAA compliance, the 2004 winter quarter results indicated "interpretation of HIPAA regulations" as the primary roadblock to compliance (where it had moved up from second place last quarter). This indicates that the findings from this study on this particular point were similar with those found on the research conducted by HIMSS/Phoenix Health Systems, as well as the fact that there is still a need for further material, explanation, and training on the interpretation of the federal regulations.

The two areas in which the respondents felt their facilities were the closest in reaching security compliance were (1) establishing policies/procedures for obtaining required business associate agreements and (2) policies/procedures for establishing physical safeguards to limit access to electronic information systems with facility access controls, workstation use and security, and device and media controls. The two areas in which they felt they were not as compliant were (1) policies/procedures for addressing security incidents (a response and reporting plan) and (2) policies/procedures for performing a periodic technical and non-technical evaluation of security practices governed by the Security Rule. This indicates that many hospitals realize the importance of establishing security policies (which must come first); however it takes longer to create policies for handling security incidents and evaluating the policies/practices once in place. The two areas in which they felt the most change was required were in changes to the budget in information systems and changes in network monitoring. It is obvious that in order to establish the policies, create the systems to implement the policies, and maintain and monitor the systems, it costs money and takes time.

In regard to physical on-site security methods, the majority of the respondents (58%) indicated they used electronic authorization for entry into secure areas and the next primary method used by the respondents (41%) was a security guard or other personnel. The study also found that 73% of the respondents used firewalls and 43% of the respondents were using virtual private networks. As reported by HIMSS and Phoenix Health Systems, in regard to transmission of secure transactions, the solutions most frequently reported were: virtual private networks, encryption, SSL web site, direct connection to third party, bulletin board system connection, secure dedicated lines, password protection, secure file transfer protocol, and authentication and access control on transactions. These are all types of security methods and devices that should be covered in information systems/information security curricula so students and individuals in business and industry can receive up-to-date training to develop the knowledge and ability to provide the security needed by organizations.

IMPLICATIONS AND RECOMMENDATIONS

While this study analyzed some issues similar to those reviewed by the Health Organizations, it focused primarily on identification of job titles and responsibilities of HIPAA officers, their perceptions regarding level of change needed to meet HIPAA security compliance, and the specific security methods and devices utilized. This study identified that many facilities were experiencing high levels of change required in IS budget requirements, network monitoring, hiring in the IS department, and changes to networking infrastructure and technologies. Therefore, there is a need for knowledgeable individuals in the field of information systems and technologies to assist those in the healthcare industry to reach HIPAA compliance. Also, the role of health information managers is changing and they are being required to understand more about information technology, data security, and management of electronic information. These individuals will continue to see their roles expand as the healthcare industry moves to the use of more electronic health records. Healthcare entities are just scratching the surface as far as changes that are expected in regard to conversion of all paper-based health records to electronic records, which is being mandated by the President to improve the quality of healthcare and reduce costs. Therefore, as hospitals are forced to meet HIPAA compliance, they may find they are more prepared for other changes. For example, the continued transition from paper to electronic health records and the interoperability of these records should be less complex, more efficient, and more secure as a result of HIPAA.

Colleges and universities must continue to focus on preparing a work force that has a strong understanding of the issues affecting all industries regarding the emphasis of privacy and security of information. Not only do those in the field of information systems and information management need to stay up with the new technologies related to the different types of security alternatives, devices, and systems; but those in many other areas of management must know how to use, implement, and manage these systems. All of these individuals, especially those in the field of business, must know how to plan, establish, implement, and manage policies for various types of organizations. Students must be made aware of the impact federal regulations, such as the Health Insurance Portability and Accountability Act, the Gramm-Leach-Bliley Act, and the Sarbanes Oxley Act, have on healthcare facilities and other organizations.

Corporations must continue to place more emphasis on importance of the establishment of privacy and security policies and their implementation and evaluation. For example, more and more companies are hiring a Chief Privacy Officer who "would be responsible for establishing clear and consistent standards throughout the organization by understanding which kinds of information are critical, how to maintain the confidentiality of the information and how to support the integrity, reliability and availability of the data" (Wilson, 2003). Educators and business representatives must work together to collaborate in preparing a stronger work force of knowledgeable individuals that can develop and implement the privacy and security policies for healthcare entities as well as other companies and agencies that must provide secure transmission of private data.

More research studies are recommended to identify the overall privacy and security needs of healthcare entities as well as other industries. These studies can examine specific policies and procedures that have been identified as "best practices" as well as reasons why various security policies, solutions, and devices are used as opposed to others. They can also look into ways to provide training for end users on how to maintain privacy and security of individual and corporate information.

REFERENCES

American Health Information Management Association. (2004). The state of HIPAA privacy and security compliance. Retrieved April 20, 2004, from http://www.ahima.org/hipaa/suvey.cfm

Fitzgerald, T. (2003, May/June). The HIPAA final rule: What's changed? *Information Systems Security*, *12*(2), 50-69.

Fitzgerald, T. (2004). The final HIPAA security rule is here! Now what? In H. F. Tipton & M. Krause (Eds.), *Information Security Handbook* (pp. 1919-1935). Boca Raton, FL: CRC Press LLC.

Healthcare Information and Management Systems Society (2004). About HIMSS. Retrieved April 24, 2004 from http://www.himss.org/asp/abouthimss_homepage.asp

Peled, A. and Troyansky, L. (2004, March). Twelve steps for compliance in a convoluted regulatory environment. *The ISSA Journal*, 8-11.

Phoenix Health Systems. (2004). US healthcare industry quarterly HIPAA compliance survey results: Winter 2004. Retrieved April 19, 2004, from http://www.hipaadvisory.com/action/surveynew/winter2004.htm

Smith, H. E. (2003, October). The HIPAA final security rule--more than a new security standard. *The ISSA Journal, 16-19.*

Wilson, M. (2003, May 1). How to ensure security compliance with HIPAA. *Computer World* [Online]. Retrieved July 15, 2003, from http://www.computerworld.com/securitytopics/ security/story/0,10801, 80812,00.html