Safe Teleradiology: Information Assurance as Project Planning Methodology

JEFF COLLMANN, PHD, ADIL ALAOUİ MS, DAN NGUYEN, MD, DAVID LINDISCH, RT

Abstract The Georgetown University Medical Center Department of Radiology used a tailored version of OCTAVE\textsuperscript{SM}, a self-directed information security risk assessment method, to design a teleradiology system that complied with the regulation implementing the security provisions of the Health Insurance Portability and Accountability Act (HIPAA) of 1996. The system addressed threats to and vulnerabilities in the privacy and security of protected health information. By using OCTAVE\textsuperscript{SM}, Georgetown identified the teleradiology program’s critical assets, described threats to the assurance of those assets, developed and ran vulnerability scans of a system pilot, evaluated the consequences of security breaches, and developed a risk management plan to mitigate threats to program assets, thereby implementing good information assurance practices. This case study illustrates the basic point that prospective, comprehensive planning to protect the privacy and security of an information system strategically benefits program management as well as system security.


Developers of automated information systems face requirements to assess and mitigate threats to the privacy and security of the individually identifiable information in their systems. For example, as part of the design and development of new information systems, United States government agencies must complete information security risk and privacy impact assessments in compliance with requirements of laws such as the Privacy Act of 1974 and the Federal Information Security Management Act of 2002 and Appendix III of the Office of Management and Budget Circular A-130.\cite{1} During the past two years, computerized biomedical devices with major operating system vulnerabilities have emerged as major threats to enterprise networks, thus provoking calls for better design as well as repair.\cite{2,3} The Department of Radiology, Georgetown University Medical Center used OCTAVE\textsuperscript{SM}, a self-directed information security risk assessment process, in an effort to design a teleradiology system that complies with the regulation implementing the security provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). This system addressed threats to and vulnerabilities in the privacy and security of protected health information (Fig. 1).\cite{4,5,7} Using the OCTAVE\textsuperscript{SM} process, Georgetown identified the teleradiology program’s critical assets; described threats to the assurance of those assets; developed and ran vulnerability scans of a system pilot; and evaluated the consequences of security breaches for patients, the teleradiology program, and Georgetown. With this information, Georgetown developed a risk management plan to mitigate threats to program assets and to avoid vulnerabilities by implementing good information assurance practices. Accomplishing these aims, however, required addressing strategic issues in the teleradiology program’s management as well as resolving specific security issues.

The OCTAVE\textsuperscript{SM} Method

OCTAVE\textsuperscript{SM} has three phases: the organizational view, the technological view, and strategy and plan development.\cite{4,5} It meets all risk assessment requirements of the National Institute of Technology and Standards and contrasts with most information security risk assessments that focus on identifying vulnerabilities in technical infrastructure only.\cite{8} Internal staff teams carry out OCTAVE\textsuperscript{SM}, thus building organizational expertise and ownership in the results. Among many other organizations, the medical services of the U.S. Army, Navy, and Air Force adopted OCTAVE\textsuperscript{SM} for all military treatment facilities to use in conducting their HIPAA security risk assessments.\cite{9}

In phase 1, organizational view, a multidisciplinary analysis team drawn from the organization runs workshops with representatives of various levels of its hierarchy, including senior leaders, operational area managers, regular staff, and IT staff. During these workshops, the analysis team elicits opinions...
regarding the organization’s critical information assets, threats to the critical assets, the relative importance of confidentiality, integrity and availability in protecting the assets, and the organization’s daily practices that support or undermine information assurance.

The analysis team follows guidance and uses various worksheets provided in a comprehensive set of guidebooks called the OCTAVESM Method Implementation Guide (OMIG) to capture information from workshop participants (for information about ordering a copy of the OMIG, go to http://www.cert.org/octave). Through extended discussion and debate, the multilevel workshops and multidisciplinary analysis team build shared consensus out of multiple and often conflicting perspectives regarding the priorities and methods of an organization’s information assurance program.

One member of the analysis team functions as a facilitator and another as a scribe. All workshops begin by identifying an organization’s important information assets, such as information, information systems, hardware, software, and people. After producing a list of 20 to 30 items, participants choose the five most important assets (such as patient information, the clinical information system, and the paper medical record) and prepare a justification for selecting each one. The process is repeated to identify threats to the important assets and to specify the confidentiality, integrity, and availability requirements for each asset. Participants then complete OMIG survey forms and engage in extensive discussion of the organization’s strengths and weaknesses in the practice of information security. Based on the Catalog of Good Practices derived from a range of information security industry sources and emerging requirements such as HIPAA, the British Standard 7799, and ISO/IEC 17799, the survey and discussion enable the participants to benchmark their organization against accepted norms of the information security industry.6,7

In many cases, the data gathered from the various constituencies will provide evidence for differing and, perhaps, conflicting perspectives on these central organizational issues. The analysis team then begins to identify and adjudicate among these different perspectives by selecting five critical information assets from among those identified in the earlier workshops and creating “threat trees” that illustrate the range of sources, access routes, motive, and outcomes of a threat. The analysis team graphs threat scenarios according to human, system, or other threat sources and physical or network access. For human threat sources, the threat trees categorize a scenario according to the actor’s status with respect to the asset (authorized or unauthorized user) and motive (deliberate or accidental breach). The process finishes by identifying the type of breach or outcome to the asset (disclosure, damage or loss, unavailability) (Fig. 2).

The analysis team documents all this information in an asset profile workbook for each critical asset.

In phase 2, the technological view, the analysis team organizes and conducts a vulnerability scan or assessment of vulnerabilities in the technical infrastructure of computerized segments of the information management system. Organizations often administer such scans as part of their routine information security program. OCTAVESM differs from most established procedures in targeting the vulnerability scans to the information systems, components, and access pathways that support the organization’s critical electronic information assets previously identified in phase 1, organizational view. The analysis team identifies the relevant infrastructure segments and key components that grant access to specific assets and, from this list, selects a sample of components for actual scanning. After receiving the results of the scan, the analysis team chooses specific technical vulnerabilities for mitigation, one part of the overall mitigation plan discussed below.

In phase 3, strategy and plan development, the analysis team consolidates, analyzes, and responds to all the organizational and technological data acquired in phases 1 and 2 to develop the organization’s information security risk management program.
At this point, the analysis team conducts the actual risk analysis; that is, it identifies the impact or consequences of breaches of its critical information assets for its customers, programs, and organization. For example, a hospital analysis team may decide that breaches of the confidentiality of its patient record would damage its reputation. It develops measures of high, medium, and low impact of a breach on its reputation. For reputation, appearing on the front page of the *Washington Post* or on CNN might constitute a high impact, appearing in the local paper might constitute a medium impact, and rumors circulating among hospital staff might constitute a low impact. Accreditation penalties, loss of patients, and loss of referring physicians represent other possible measures of reputation. Other measures of risk include effect on the life or health of patients, staff productivity, fines and legal penalties, and finances.

After describing risk evaluation criteria, the analysis team returns to the threat trees for each asset and ranks the breaches according to their potential impact. In Figure 2, for example, the branch indicating “outsider deliberately modifying patient information” might warrant a high impact for several reasons. The hospital’s reputation might grievously suffer if news of the altered patient information hit the media. The patient could suffer serious harm. The hospital could sustain fines, legal penalties, and accreditation penalties. The analysis team completes this process for all assets and all relevant threat trees.

As the final step, the analysis team actually builds a response to the implications of the data; that is, the information security risk management plan. The plan includes three parts: an action list, mitigation plans, and a protection strategy. The action list includes items for immediate repair that generally require no new staff, policies, or capital investment. An example might include ending access privileges of terminated employees or changing default passwords. The mitigation plans focus on significant threats to the critical assets and include methods to recognize, resist, and recover from a breach. For the hacker scenario, the analysis team may propose to install a perimeter defense to recognize and resist unauthorized access, including a network firewall and intrusion detection devices. The complete set of mitigation plans should have a broad impact, providing protection for an organization’s secondary as well as critical assets.

In contrast to the mitigation plans that focus on critical information assets, the protection strategy focuses on improving an organization’s strategic and operational information security by sustaining good practices and reforming poor practices. From the strategic perspective, the analysis team may determine that the organization’s security training and awareness program lacks a discussion of HIPAA and decide to purchase a commercial HIPAA training package for distribution on its Intranet.

The Catalog of Good Practices fundamentally links information security management to management of the organization as a whole. Well-managed organizations tend to support sound information assurance
programs. From the perspective of planning, however, the Catalog of Good Practices suggests that organizations may use the process of designing a well-managed information assurance program to develop a sound approach to general program management, particularly when designing a new information system such as a teleradiology program.

Description of Case Study

For planning its teleradiology program, Georgetown tailored the standard model by conducting all steps of the process using members of the analysis team only, a recommended approach for small organizations. The team included the physician director of the teleradiology program, two radiology administrators, a radiological technologist, and information technology specialist as well as a facilitator. Acting on the results of the evaluation required meeting with many people from the Department of Radiology, Georgetown University Hospital, MedStar (the owner of the hospital), Georgetown University information systems, and the teleradiology vendor as well as the common carrier. The OCTAVE®-specific meetings required about 100 total hours by the seven team members but yielded results far beyond the scope of what is usually considered information security. In addition to identifying important information security issues, the OCTAVE® process provoked reevaluation of the teleradiology project’s mission, support requirements, and overall project management as well as its technical infrastructure. Thus, the time spent on security constituted an investment in the project’s overall success.

Active participation of the members of the Georgetown multidisciplinary analysis team varied in response to predictable and unpredictable contingencies. During the course of the teleradiology planning OCTAVE®, the hospital suffered a major flood, the Joint Commission of American Hospital Organizations held an inspection, staff physicians required emergency coverage, and daily tasks demanded urgent attention, all at times of scheduled meetings. During phases 1 and 2, redundant representation in physician and administrative roles enabled meetings to occur without all members in attendance. A core group of members scheduled and attended all meetings. With only one exception, the Georgetown analysis team never met without the physician director. Of the seven original members of the team, only one failed to attend any meetings and was replaced.

Georgetown’s experience illustrates a general point: Representatives of an organization’s core business domain such as physicians and other health care providers face serious barriers to participation in OCTAVE®. On the one hand, few clinicians will identify themselves as “experts” in information technology or information management, least of all information assurance. When appointing such individuals to the OCTAVE® analysis team, the organization should emphasize its interest in eliciting their disciplinary expertise and their perspective on information management as they have developed it in their daily work. Through the OCTAVE® process, the analysis team will gather their disciplinary, work-based expertise, compare it with other perspectives, and attempt to reconcile discrepancies in the service of the organization’s greater information assurance program. Furthermore, clinicians or other domain experts on the analysis team will learn about information assurance as they study, implement, and analyze the results of various steps of OCTAVE®. On the other hand, clinicians and other domain experts often face rigid and high-productivity expectations that preclude other work. Given these pressures, hospital leaders and staff may resist inaugurating a lengthy process such as OCTAVE®. Deciding to allocate the tasks to a single department such as information technology to avoid productivity losses in the core business and administrative domains will fundamentally undermine the effectiveness of the OCTAVE® results because they will not reflect the necessary process of articulating and adjudicating among diverse perspectives on information use and management in the organization. Thus, when initiating an OCTAVE® process, organizations must officially acknowledge the implications of membership in the analysis team for participants’ other work.

In phase 1, organizational view, the Georgetown team identified the teleradiology program’s critical assets and threats to their confidentiality, integrity, and availability. The Georgetown team eventually selected five from an original list of 20 assets as critical, including patient images, server hardware and software, client hardware and software, information technology support, and radiologists themselves. This process immediately expanded their vision of the issues at stake in the planning process, particularly with reference to threats to the radiologists and information technology support. By considering how to protect the availability and effectiveness of the radiologists and information technology support, the team addressed many fundamental issues in program management, including the basic mission of the teleradiology program. The teleradiology program was intended to provide immediate support to the work of radiology fellows, consulting radiologists, and referring physicians, particularly at night and on weekends. When the OCTAVE® process began, the radiologists on the team perceived teleradiology as “supplementary” to the existing work process. Examining the question of threats to the availability and consequences of losing technical support for users, however, provoked a serious discussion about exactly what the department expected from the teleradiology program and what it was willing to pay to achieve those expectations. As a supplementary program, teleradiology could withstand interruptions in the availability of technical support. If the system crashed at odd hours of the night or weekend, the radiologists would enter a “trouble call” and travel to the hospital to render their consultation with technical support addressing the problem on the next business day. As a “mission critical program,” however, teleradiology could not withstand overnight interruptions and required technical support at all hours, including nights and weekends.

These discussions during the use of OCTAVE® caused the department to change its assessment of teleradiology from supplementary to mission critical. After estimating the cost of providing 24-hour, 7 days per week coverage, however, the department realized that it could not afford continuous technical support and adopted a program that provides 12-hour coverage everyday from 8:00 AM to 8:00 PM. While not avoiding travel in the night given a system crash, it does avoid downtime for more than a few hours in most cases. In particular, a crash on the weekend does not leave the system unavailable until Monday morning. Balancing financial considerations with mission expectations also
precluded solutions such as hardware backups for the one server and five laptops. The five on-call radiologists take all laptops home at night. If the server or a laptop has hardware or software problems, technical support repairs them but does not provide substitutes.

The Georgetown team conducted the OCTAVE™ phase 2, the assessment of vulnerabilities in the technical infrastructure, on a pilot teleradiology system of one server and two laptops. This process identified several important vulnerabilities in the teleradiology system and the MedStar security infrastructure whose resolution produced new working relationships among program, hospital, and network staff as well as technical improvements and system redesign. The teleradiology program's planned use of the Internet posed a risk to the confidentiality and integrity of the patient images and compliance with a proposed HIPAA requirement to encrypt protected health information. MedStar, Georgetown University Hospital's parent system, was in the process of planning and deploying a virtual private network (VPN) to protect the corporate network. The teleradiology program could exploit this technical development as part of its mitigation plan to protect patient images in transmission and, in combination with MedStar peripheral defenses (such as the Georgetown University Hospital firewall), protect access to the teleradiology server. Like the teleradiology program, however, the VPN program was under development. The teleradiology pilot became the pilot for the VPN program. It identified and prompted elimination of bugs in the VPN deployment, e.g., improper network configuration that denied access to the teleradiology server and slowed access speed.

Georgetown discovered technical approaches in the teleradiology application that did not comply with its operational and security requirements. The system did not initially audit and log all accesses to patient data or require periodic password change. Moreover, the system only permitted two levels of access: user and administrator. Such a two-tiered access control system does not match the routine work process of health care. In response to the OCTAVE™ analysis and HIPAA, the vendor installed access audit and log function, expanded the range of access control levels, and implemented mandatory password change at regular intervals. Because the vendor looks to Georgetown for expert advice on operational matters, it adapted the technology to conform to more stringent requirements. This resulted in technical innovations in the product and a more secure system for Georgetown.

The pilot project also emphasized an elementary fact of using public networks for corporate business: multiple organizations have immediate responsibility for ensuring the reliability of service. In Georgetown's case, these organizations included MedStar, the teleradiology system vendor, and the VPN vendor, to say nothing of the Internet service provider and communications company. In organizational terms, developing technical support required determining who bears responsibility for troubleshooting and adjudicating among all these players in case of trouble or a system failure. Testing the teleradiology pilot established effective working relationships among the program's technical support team, MedStar and Georgetown information technology staff, the VPN vendor, and the teleradiology vendor, thus laying the groundwork for crisis management when necessary in the future.

In phase 3, strategy and plan development, the Georgetown analysis team truly confronted the organizational dimension of the planning process in several important ways. Conducting the risk analysis required assessing the impact of breaches of confidentiality, integrity, and availability on patients, the teleradiology program, Georgetown University Hospital, and MedStar. Georgetown learned that this requires full participation of all members of the team. Without the administrative and clinical perspectives regarding the implications of a breach for organizational reputation, staff productivity, fines, etc., the team could make no informed decisions about mitigation plans. As a result, the team postponed meetings when contingencies forced critical members to attend to other duties. More fundamentally, determining the criteria for evaluating high, medium, and low impact of a breach drew all members of the Georgetown team into an analysis of the implications of information assurance for overall program management. This analysis transformed the OCTAVE™ from a bureaucratic exercise into a genuine tool for enhancing Georgetown's organizational capability. The final step in the process, the development of a protection strategy, includes two critical components: developing a plan to mitigate threats to the critical assets and developing a program to enhance organizational practices in information assurance using the OCTAVE™ Catalog of Good Practices. During discussion of patient images, the Georgetown team decided that the original plans to use the radiologists' own home computers as teleradiology clients posed unacceptable threats to the confidentiality and integrity of the images. In addition, the teleradiology technical support team did not think it could easily service or impose restrictions on the use of the radiologists' personal property. Avoiding these problems required purchasing workstations dedicated solely to the teleradiology program and thus spending scarce departmental funds. To address this question, the physician director of the teleradiology program called a meeting of representatives of the radiology department, hospital information technology, and MedStar administration. After a thorough discussion of the threats to the patient images from using the radiologists' home computers, the radiology chairman authorized purchasing laptops from departmental funds with full concurrence of MedStar's administration.

Discussion of mitigating threats to the physical security of the laptops produced additional innovations in program management. Using laptops instead of the radiologists' home computers entailed transferring machines from one radiologist to another as responsibility for night and weekend call rotated. The Georgetown team established a transfer protocol requiring each radiologist to log in and log out of a journal as they exchanged the laptop. Because one laptop was assigned to each of five departmental divisions, the physician director of each division accepted ultimate responsibility for safely transferring the laptop. The radiologists also initially intended to use one shared password for all the laptops. Review of impending HIPAA requirements for unique user identification justified adopting individual log-ins for each radiologist. The Georgetown team drafted a code of safe practices that encouraged radiologists to take personal responsibility for the laptop's protection, including following the check in/check out protocol, avoiding locations subject to water damage, always using a surge protector, avoiding general use areas
such as their family room, working in secluded areas while being aware of prying eyes, avoiding food and spills near the laptop, not using screen capture to store the displayed images, and storing the laptop safely during periods of rest or transport. In addition to enhancing protection of the laptops, these measures created a shared interest among the teleradiology program management, departmental division management, and the individual radiologists in jointly assuming responsibility for the program’s operation.

From a planning perspective, reviewing the Catalog of Good Practices refocused the entire process from the teleradiology system of hardware and software to the management of the teleradiology program. In a conventional OCTAVE℠, workshop participants in phase 1 complete a survey based on the Catalog of Good Practices, eliciting their perspectives on the organization’s current state of practice. Because the teleradiology program did not yet exist, the Georgetown team used the Catalog of Good Practices and the draft HIPAA data security rule as prospective guides to planning policies, procedures, and practices that the program should adopt. From this, the team produced the Teleradiology Information Security Policy (available at http://isisit.georgetown.edu/telerad) and finalized the teleradiology management process. Successful completion of this step in OCTAVE℠ as well as the risk assessment as a whole grounds Georgetown’s claim that its teleradiology program complies with the core expectations of the HIPAA Security Rule.5

Georgetown used the training of prospective teleradiology users, including the radiologists, radiology residents, and relevant radiology staff, as an opportunity to present the teleradiology program’s operation, security, and management as a coordinated whole. The training sessions lasted for approximately 90 minutes. After hearing the Director of Teleradiology explain the origins, funding, planning, and purpose of the teleradiology program, the teleradiology users received didactic and hands-on training in use of the teleradiology software from the system vendor. The training sessions closed with an overview of HIPAA Security and a detailed discussion of how the teleradiology program complies with the new regulations. This twofold approach to teleradiology security training reminded the physicians, technologists, and administrators of the new regulations and explained and justified the security measures of the teleradiology program. All prospective teleradiology users signed the Teleradiology Protection Statement.

Conclusion
Organizational theory cautions against too much optimism about the long-term beneficial effects of planning. Snook10 emphasizes how practices gradually drift from written policies and procedures as individuals, groups, and organizations adjust their work to its context. That being said, using a comprehensive risk assessment method during system design potentially facilitates a “good launch” that should enhance an organization’s ability to manage complex health information systems safely and in compliance with regulatory regimes such as HIPAA.11–16 A comprehensive, prospective risk assessment such as OCTAVE℠ engages senior leaders in support and execution of the process; develops a multidisciplinary team from the organization to plan, execute, and evaluate the results of the risk assessment; solicits perspectives on health information assurance practices from all levels of the organization (senior leaders, middle management, general staff, and information technology staff); creates processes for developing a shared consensus on information risk management; trains participants in information assurance; and establishes data about an organization’s information security risks for ongoing study and learning. To gain these benefits, health care organizations must assemble and adequately support skilled, knowledgeable participants drawn from their key constituencies, including health care providers, administrators, and information technology. Sustaining these gains will depend on integrating information security risk management into the ongoing management of health information systems instead of leaving it at the planning doorstep upon deployment.

References
1. Office of Management and Budget, Circular A-130, Appendix III.