Handling a Security Breach: Lessons Learned

Save to myBoK

by Michelle Dougherty, RHIA

Consider this: your facility just received a call from a reporter asking for a comment. He's writing an article on a hacker who accessed your network, downloaded patient medical information, and distributed copies to the press.

If your facility experienced a security incident—a breach, a leak, a stolen laptop or PDA—would you be prepared to handle the situation? Tom Martin, chief information officer at the University of Washington Academic Medical Center, was forced to confront the above scenario after a hacker accessed a database of patients' medical information. His experience can help others in the healthcare industry prepare for a similar incident.

A Hacker Attacks

A hacker gained access to a portion of the university's network through one of the academic departments in June 2000. At the end of the month, the IT department discovered strange log-in activity. Campus forensics identified the entry as an Internet service provider in the Netherlands.

After investigating the activity, the university decided not to report the incident to the FBI because damage (the key criteria for reportability) could not be proven. There was no proof that confidential patient information had been accessed.

The Media Descends

Six months after the incident had been identified and dealt with, a reporter from *SecurityFocus*, an Internet newsletter, contacted the university for comment on an article focusing on the hacker attack. The university's response was that it was investigating the incident and taking it very seriously. Within minutes, the article "Hospital Records Hacked" appeared on the SecurityFocus.com Web site, saying that a hacker "took command of a large portion of the university's internal network" and that the computerized admissions records for 4,000 heart patients had been downloaded. The article also included a quote from the supposed hacker stating, "All the data taken from these computers was taken over the Internet. All the machines were exposed without any firewalls of any kind."

Later that day, MSNBC called for comment. By the next morning, calls were coming in from major East Coast media and all major media in the Seattle area.

The University Responds

The university issued a formal statement acknowledging that a hacker gained entry to the medical center's network but denied that the hacker took control of parts of the medical center's internal network. The statement noted that there had been no evidence of confidential data being obtained and that no one had gained entry into the separate, highly confidential patient-care computer system. At that point, a crisis management team was established with members from senior management.

Later that day, two news organizations faxed evidence that confidential information had been obtained. The information came from a cardiology database outside the main medical records system and contained identifying information and social security numbers. The university issued a second statement to acknowledge the receipt of the evidence, reiterate that the main electronic records system had not been breached, and report that the FBI was involved due to the tangible evidence of damage.

By the end of the day, it was clear that the breach was very serious and the crisis management team was broadened to include media relations, information systems, hospital leadership, and telecommunications. The team assessed the risk of the situation, identified action items, and assigned duties to team members.

Internally, campus leadership and employees were informed and kept up to date through e-mailed Q&A documents and statements. In addition, the government relations staff kept legislators informed and the Association of Academic Medical Centers was contacted for assistance. Externally, a news conference was held with physicians and the CIO to provide details to media and ask for assistance in publicizing medical center contact and Web site information for the public to access.

The university set up special information telephone lines for the public that were manned 10 hours a day for the first week. Trained public relations specialists from an external firm and university managers handled about 450 phone calls mainly dealing with identity theft issues. A letter was sent to each living individual in the stolen database explaining what had happened, detailing the information stolen, and offering advice on identity protection.

Lessons Learned

Martin identified some of the university's successes in dealing with this event. They included:

- the decision to keep the focus on the patients and what could be done to inform, reassure, and advise them
- the leadership response in handling the media and maintaining a no-blame approach to the event
- the incident response process and the crisis management team's involvement
- the technical staff's response to the intrusion and their actions to correct the problem

At the same time, Martin learned some valuable lessons in terms of dealing with the press. Be careful what you deny, because that may be used against you. Be clear about what is unknown and avoid details. Further, Martin realized that the security and privacy officer should have coaching on how to handle the media in situations like this.

A number of changes have occurred at the University of Washington since the security breach, including upgrades to the technology infrastructure and centralization of security. Additionally, the event helped sharpen the organization's understanding of HIPAA. Staff don't ask why it is important to comply—they've seen the consequences first hand.

One final lesson: regard security as a risk management activity because these events will happen despite all the best efforts. A good security program should include prevention, detection, and response. Breaches of patient information by a healthcare organization are very newsworthy, so be prepared in case it happens to you.

Reference

Poulsen, Kevin. "Hospital Records Hacked." *SecurityFocus*. December 6, 2000. Available at www.securityfocus.com/news/122.

Michelle Dougherty *(michelle.dougherty@ahima.org) is an HIM practice manager at AHIMA.*

Article citation:
Dougherty, Michelle. "Handling a Security Breach: Lessons Learned." *Journal of AHIMA* 73, no.2 (2002): 54-55.