Cybersecurity Insurance: Considering Coverage for Data Breaches

By Barry S. Herrin, CHPS, JD, FACHE, and Frankie T. Jones, Jr., JD

In 2009 the average cost per incident of a data breach in the United States was $6.75 million.[1] Mark Bregman, executive vice president and chief technology officer at Symantec Corporation, cited this statistic during his testimony before the Senate Subcommittee on Consumer Protection, Product Safety, and Insurance concerning the Data Security and Breach Notification Act of 2010.

Introduced in August 2010 by Senator Mark Pryor (D-AR), the bill aims to protect data containing personal information and address the growing problem of data security breaches across all sectors. It echoes provisions in the HITECH Act that increase the penalties for breaches of protected health information.

With the number of reported breaches rising, federal scrutiny intensifying, and penalties increasing, healthcare providers may want to explore cybersecurity insurance as part of their overall strategy to prevent and manage data breaches.

Security Breaches on the Rise

According to Verizon, more electronic records were breached in 2008 than in the previous four years combined. In fact, since 2005, more than 365 million records containing personal information have been exposed by electronic security breaches.[2] The number of electronic records containing personal information exposed by hackers increased from 35 million records in 2008 to 220 million in 2009.

In addition, electronic data breaches of records containing personal information are becoming more expensive. From 2005 to 2008, the average cost of a data breach rose by $2.25 million. Beyond the direct costs incurred in resolving such breaches, organizations also suffer reputational damage and loss of customer confidence. In 2008 organizations that experienced data breaches averaged $4.6 million in lost business as a result of the breach.[3]

Concerns over data breaches are particularly pertinent in the healthcare sector. In 2009 healthcare ranked second only to the education sector in terms of known data breaches that could lead to identity theft.[4] The pervasiveness of data breaches is even more important given the requirements and penalties imposed by HIPAA as amended and amplified by the HITECH Act.

The HIPAA privacy rule establishes the national standards for use and disclosure of an individual's health information and sets civil money penalties for noncompliance. Initially civil penalties were limited to no more than $100 per violation and were capped at $25,000 per calendar year. However, the HITECH Act significantly increased the civil penalties that healthcare entities may face.

Pursuant to the HITECH Act, civil penalties under HIPAA now range from $100 to $50,000 or more per violation and have a much higher cap of $1.5 million per calendar year. In addition, in the event of certain types of breaches of unsecured protected health information, healthcare organizations are required to notify each individual whose unsecured protected health information has been accessed, acquired, or disclosed as a result of such a breach, as well as the government and-in breaches of 500 or more records-the local media.

The Data Security and Breach Notification Act of 2010 would require all organizations that own or possess data containing personal information to establish and implement policies and procedures to protect such personal information, similar to HIPAA requirements. Organizations that have suffered an electronic data security breach also would be required to notify persons whose records were compromised, again similar to HIPAA.

However, the bill would assess additional penalties on organizations that have experienced a security breach. Such organizations would have to provide each individual whose information was included in the security breach with a credit-monitoring service for two years after the breach at no cost to the individual. Moreover, entities may face penalties up to $5 million per violation.

The bill has been referred to the Senate Commerce, Science, and Transportation Committee. When the Senate reconvenes, the committee will determine whether to report the bill.

Cybersecurity Insurance

Given the threat of electronic data security breaches and the increasing size and scale of costs and penalties associated with such breaches, healthcare organizations may want to consider investing in cybersecurity insurance.

Common cybersecurity policies include coverage for hazards such as data privacy loss and repairs to company databases after system failures. Broader policies include coverage for costs of notifying customers in the event of a breach as required by the HITECH Act and loss of income from site failure.

Some policies even provide for crisis management coverage, including hiring an emergency public relations team and monitoring credit for affected persons (as would be required by the Data Security and Breach Notification Act of 2010). And some cybersecurity policies provide coverage for the acts of "rogue" employees in the inappropriate or even willful release of patient health information. Traditional liability policies might not cover deliberately inappropriate or illegal employee actions.

HIM Contributions to Cybersecurity Decision

Because they manage protected health information privacy, HIM professionals have a role in a facility's consideration of cybersecurity insurance.

HIM professionals know the risks associated with data breaches and inappropriate uses and disclosures, and they are charged with managing employees whose rogue acts might expose the healthcare provider to risk. In addition, HIM professionals are generally the members of a provider's administrative team that work most closely with the business associates that provide services utilizing protected health information and thus would be in the best position to know what risks exist in those relationships.

When making this decision, organizations may need to obtain the privacy and security policies and procedures implemented by business associates and make those available to the provider's insurance underwriters. HIM professionals (in cooperation with the provider's counsel) will be in the best position to know whether these policies and procedures are compliant and provide adequate coverage of reasonably anticipated problems. To the extent that a provider's insurance coverage did not reach the actions of business associates, HIM professionals should insist that all business associates obtain and maintain such insurance, adding the provider as an additional insured.

Cybersecurity insurance should be included as a part of a company's overall strategy to avert breaches before they occur. Preventive measures, such as stronger security protections, not only provide for a more comprehensive strategy, but also allow for lower insurance premiums.

With a strong preventive strategy and cybersecurity insurance, healthcare providers can effectively decrease the likelihood of breaches, while decreasing the impact of costs and penalties associated with these breaches should they occur.

Notes

1. Ponemon Institute. "2009 Annual Study: Cost of a Data Breach." January 2010. Available online at www.encryptionreports.com/download/Ponemon_COB_2009_US.pdf.
2. Verizon. "2010 Data Breach Investigations Report." Available online at www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf.
3. Symantec. "Symantec Internet Security Threat Report: Trends for 2008." April 2009. Available online at http://eval.symantec.com/mktginfo/enterprise/white_papers/b-

whitepaper_exec_summary_internet_security_threat_report_xiv_04-2009.en-us.pdf.
4. Open Security Foundation DatalossDB. Available online at http://datalossdb.org.

References

"Cyber Security: Data Breach Insurance Gains in Popularity," *Bank Technology News*, June 2007. Available online at www.americanbanker.com/btn_issues/20_6/-314043-1.html.

"Cybersecurity Insurance Gains More Adherents." *Homeland Security Newswire*, June 24, 2010. Available online at http://homelandsecuritynewswire.com/cybersecurity-insurance-gains-more-adherents.

Data Security and Breach Notification Act of 2010. Available online at www.govtrack.us/congress/bill.xpd?bill=s111-3742.

DuBois, Shelley. "Electronic Medical Records: Great, but Not Very Private." *Fortune*, October 6, 2010. Available online at http://money.cnn.com/2010/10/06/technology/electronic_medical_records_safety.fortune/index.htm.

Risen, Tom. "Can Insurers Protect the U.S. from Cyber-Attack?" *National Journal Online*, February 10, 2010. Available online at www.nextgov.com/nextgov/ng_20100210_8138.php.

US Department of Health and Human Services. "Summary of the HIPAA Privacy Rule." Available online at www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf.

Barry Herrin (barry.herrin@smithmoorelaw.com) is a partner in the Atlanta office of Smith Moore Leatherwood LLP. Frankie Jones (frankie.jones@smithmoorelaw.com) is an associate in the firm's Greensboro, NC, office.

Article citation:
Herrin, Barry S.; Jones, Frankie T. "Cybersecurity Insurance: Considering Coverage for Data Breaches" *Journal of AHIMA* 82, no.1 (January 2011): 36-37.