

RISK FINANCING

Dealing with cyber risk: Closing the gaps in protection

By Mark Silvestri

FORWARD

Healthcare organizations are exposed to increasing risks from data security breaches and identity theft. Traditional insurance policies were not designed to respond to these risks, but in recent years, cyber-insurance policies have been developed. These new policies vary greatly with respect to coverage, limits, exclusions and definitions. To ensure that an organization has the insurance protection it needs, risk managers should be aware of the coverage gaps in both traditional and cyber-insurance policies.

INTRODUCTION

Ten years ago, few healthcare executives contemplated the risk of lawsuits from patients whose financial or protected health information was compromised by a data security breach. Nor did they envision defending a privacy regulatory proceeding or contemplate providing notification to patients, regulators and business associates in the wake of a breach.

Today, these risks have become pervasive, leading to the development of a broad range of new insurance products, often referred to as cyber insurance.

Due to their increased reliance on electronic medical records and electronic data-storage systems, many healthcare institutions are adding cyber coverage to their insurance programs. However, these policies vary greatly in their coverage terms. Rather than filling the gaps left by traditional insurance, they may be creating a false sense of security.

This article explores emerging cyber risks, as well as the coverage gaps existing in both traditional insurance programs and cyber-insurance products. An accompanying sidebar explores the changing landscape of privacy regulatory compliance risk for healthcare organizations.

Coverage gaps

Cost of patient notification. Forty-five states have laws that mandate notification of patients whose confidential data may have been compromised. Organizations that have experienced a data security breach also may be required to pay for credit monitoring on behalf of patients who have been affected by the breach. Apart from statutory obligations, protecting an organization's reputation is reason enough to respond promptly and professionally to a breach. However, the costs of patient notification and other damage control activities are not covered by traditional general liability and property insurance products.

Invasion of privacy. In most general liability policies, "invasion of privacy" is defined as oral and written publication of confidential information. Because the unauthorized disclosure of data in a hacking incident or a lost laptop does not involve any kind of intentional publication, such losses may not be covered. In other words, there could be a critical gap in an organization's insurance protection from liability arising from privacy breaches involving medical records, electronic data-storage systems and patient financial data.

Theft of confidential information/intellectual property. The theft of confidential data by hackers or disgruntled employees will probably not be covered by property or crime/fidelity insurance policies. As a general rule, these policies apply to theft of tangible property. If appropriately endorsed, crime policies may extend coverage to include theft of the insured's information. However, they typically will *not* cover the liability exposure if confidential information of a third party is stolen while in the insured's possession. A significant coverage gap thus arises as many healthcare institutions have third-party confidential information in their custody, for instance, clinical trial data of a biotechnology or pharmaceutical firm. The economic consequences of the loss or compromise of such data could be significant.

continued on next page

Published content. Until recently, most Web sites represented electronic versions of promotional brochures. As such, material published on these Web sites was typically covered against claims of libel or copyright/trademark infringement under the advertising injury coverage of general liability insurance policies. Now, however, it is not unusual for healthcare organizations to publish materials such as health information, advice and research reports. Web sites and blogs may be used to facilitate patient-clinician interaction. Because this type of content transcends the definition of “advertisement” in most general liability policies, claims arising from it may not be covered. Content that infringes on copyrighted material, including unauthorized hyperlinks, or that may be viewed as providing medical advice could result in uninsured losses.

Emotional distress. According to a 2003 survey by the Identify Theft Resource Center,(1) the emotional impact of identity theft is profound – similar in many respects to that of a violent crime. Moreover, privacy breach lawsuits typically allege damages for mental anguish, embarrassment or stress. However, many general liability policies cover emotional distress only if it is associated with physical injury. Because physical injury does not result from privacy breach, such damages may not be covered.

Viruses/malicious software. Property insurance policies may not cover damage to data caused by hacking or viruses. As previously mentioned, property insurance generally applies to tangible property, not intangible data. In addition, property insurance typically responds to losses resulting from wind, fire, smoke, explosion and other traditional causes of loss. Therefore, if a virus destroys patient records or billing data, repair costs of that damage may be borne entirely by the healthcare organization.

Similarly, most traditional general liability policies would not protect an organization from third-party claims as a result of damage to its own data.

All this is to say that traditional insurance responds primarily to traditional claims arising from bodily injury, property damage and personal and advertising injury. Network breaches, hacking and stolen laptops probably would not trigger the coverage healthcare organizations need in the new world of privacy and data security risk.

Cyber insurance: Buyer beware

Cyber-insurance policies are designed to fill the coverage gaps left by traditional business insurance, and thereby offer necessary protection. However, these policies vary greatly with respect to coverage, limits, exclusions and definitions.

To ensure that an organization has the protection it needs, risk managers should consider the following general guidelines.

- o **Inquire about policies that cover privacy injury resulting from unauthorized use or disclosure** of *any and all* private information in the organization's care and custody. Some policies contain restrictions that limit protection to online and Web site activities.

However, privacy risk transcends network security. Nearly 70 percent of all privacy breaches involve compromise of confidential information housed in traditional channels. According to a 2005 study by the Better Business Bureau,(2) these include stolen briefcases and theft of

mail or printed documents. In view of this risk, a policy that responds to breaches involving both online and offline information will provide optimal coverage. In addition, a policy that guards against a broad range of perils, from lost or stolen laptops to network hacking will offer the maximum protection.

With respect to laptops, cyber insurance should protect an organization from breach of privacy claims resulting from theft or loss of ALL removable media, including thumb drives, personal digital assistants, tapes, discs and even paper records.

This coverage should apply to any location where the media may be lost or stolen, whether at the office, on the road or at an employee's home.

- **Many policies purport to provide coverage for complaints alleging failure to comply with applicable privacy laws,** such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Gramm-Leach-Bliley Act of 1999 or various state privacy laws. However, some of these policies contain exclusions that deny coverage for failure to abide by the requirements set forth in these statutes. For example, claims alleging failure to provide opt-out privileges from data collection may be excluded from coverage.

In other words, when a policy says it furnishes coverage for non-compliance with privacy law, risk managers should review the policy with their insurance professionals for exclusions that limit the coverage. In addition, recognize that exclusionary language also may be placed in the definitions, conditions and insuring agreement, not only in the exclusions provisions of the policy.

- **An estimated 30 to 40 percent of all privacy breaches involve third parties** that have compromised confidential data belonging to their clients.(3) This statistic reflects a serious risk for healthcare organizations that may employ vendors to digitize paper medical records or contract with data archive companies and/or data destruction vendors.

Risk managers should review the policy with their insurance professionals for exclusion that limit the coverage.

Therefore, a policy that covers an organization's liability arising out of data security breaches involving third parties will offer maximum protection against this exposure. In addition to insurance coverage, risk managers should require third parties to provide a signed agreement regarding the appropriate use of their organization's information. The agreement should contain indemnification/hold harmless provisions from claims arising from breaches in the third party's operations.

- **Alleged violations of privacy law are complex and costly to defend.** Hence, cyber-insurance protection should provide full policy limit coverage for legal defense. Policies also should help to defray the costs of remediating a compliance deficiency. In these matters, no formal legal action is instituted, but the regulatory agency establishes a "cure" period within which to fix the problem. Risk managers should exercise caution regarding policies with limitations on defense obligations, restrictions on laws that are covered, or exclusions for actions by certain regulatory authorities. Such restrictions are out of step with the current landscape of privacy risk.

The exponential increase in privacy laws has set the stage for more enforcement actions in more jurisdictions. (See

accompanying sidebar.) Therefore, coverage limitations for regulatory defense are worrisome. An inadequate defense that results in an adverse regulatory finding will probably lead to private causes of action that may become indefensible.

- **Inquire about policies under which the insurer has a duty to defend,** not simply a right to defend. With the former, defense costs are covered as they are incurred. With the latter, the insured organization is required to pay defense costs upfront, which will be reimbursed by the insurer upon conclusion of the litigation.

Another advantage of duty to defend policies is that cyber insurers typically have access to legal counsel experienced in privacy regulation and law, as well as computer forensics experts to support a strong defense.

- **If a healthcare organization's data security is breached, notifying all affected parties, not only patients, can be time-consuming and costly.** Therefore, cyber insurance should cover, at a minimum, the costs of compliance with "duty to notify" laws. Moreover, this coverage should be triggered not only by statutory duty but by any incident with the potential to harm the orga-

Online Compliance Training

authored & updated by **PRICEWATERHOUSECOOPERS** ■ developed & delivered by **eHealthcareIT**

OVER 98 DEPARTMENT SPECIFIC COURSES

Admissions & Registration (3)
 Allied Health Services (9)
 Patient Relationships
 HIM Coding Compliance (3)
 HIM General Compliance (2)
 HIM Compliance Management (3)
 Home Care (3)
 Home Health (3)

Hospice (4)
 Home Medical Equipment (2)
 Intro to the Regulatory Environment (3)
 Laboratory Administration (3)
 Coding & Pricing in the Laboratory (2)
 Processing Laboratory Orders (3)
 Management Responsibilities in the Health Care Environment (4)

Nursing Documentation (4)
 Patient Financial Services (4)
 Physician Coding (2)
 Physician Documentation (9)
 Skilled Nursing (5)
 Laboratory General Compliance (2)
 EMTALA (3)
 HIPAA (13)

Additional online training curriculums available include: Coding, Disaster Preparedness, Clinical Simulations, CE's & Joint Commission Standards, HFMA: Finance, Billing, Avoiding Claims Denial, and Cost Control

CLIENTS RECEIVE:

- Monthly virtual roundtables with PricewaterhouseCoopers Healthcare Advisory practice consultants & your compliance peers
- Interactive courseware with case studies & scenarios
- Option to utilize your facilities' current eLearning system or eHealthcareIT's award winning eLearning system that features discussion forums, compliance alerts, and multiple communication tools targeted to your learners
- Subject matter experts with functional and operational expertise: PricewaterhouseCoopers

COURSEWARE DESIGNED FOR THE FOLLOWING AUDIENCES:

Coders • Billing/Financial Services • Pharmacy • Admitting Home Care • Nurses/Patient Care Providers
 Finance • Physicians-Employed • Discharge Planning • Compliance/Audit Laboratory, Hospice
 ER Support Staff • Cardio Services • ER Nursing • Therapies • Registration • HIM • Physicians-Not Employed
 • Volunteers • Board Members • Skilled Nursing/Long Term Care • Nursing Management



eHealthcareIT
 eLearning & IT Solutions

For further information or to arrange a product demonstration please email: info@ehc.it or call 1-800-806-0874
www.ehealthcareit.com

nization's reputation. In addition, a policy should either provide breach response services or cover their costs. Valuable services include media relations, outreach to regulators, call centers to respond to inquiries from affected parties, as well as identity theft management and credit monitoring for these parties. Not only can these services begin to repair an organization's reputation, they can help to avert potential identify theft by criminals using the lost or stolen information and any ensuing litigation brought by victims.

- **Beware of policies that seem to offer very high limits for credit monitoring or credit protection** for “serious breaches” or “serious security failures.” Some policies purporting to offer very high limits actually place a cap on the per person cost for credit monitoring services. This cap effectively reduces the available coverage limit. Also, meaningful coverage responds before the data compromised in a breach can be exploited by unauthorized recipients. Coverage should be designed to alert potentially affected individuals that they may be at risk and should help them undertake precautionary measures. Some of these “high limit” policies also have coverage triggers requiring evidence that a criminal has actually obtained the breached information and will exploit it for illicit purposes. Some require evidence of unauthorized activity in affected individuals' accounts. Producing such evidence may not even be possible. Moreover, time is of the essence in taking precautionary measures. Offering to provide credit monitoring services after criminal activity has been established will not minimize the possibility of being sued. Once individuals affected by such acts have been harmed, they may sue regardless of an organization's offer of remediation services.
- **Cyber claims may arise regarding information collected using cookies, bugs, key-stroke loggers or other spyware** that can be secretly installed on an organization's network by third parties. Policies that exclude these data collection mechanisms may create significant exposure.
- **Risk managers should seek affirmative coverage for claims** arising from their own or a third party's inability to access or to rely upon the information provided by the organization's network. Care delivery and care quality management have become increasingly reliant on electronic medical records and other online resources. If others cannot deliver care because they cannot rely on an organization's network or data, severe economic consequences may result. Or, if the organization must turn away patients due to network and data issues, there may be a loss of income. An insurance policy that responds to both scenarios is needed.

- **Consider the services that come with a cyber-insurance policy.** As noted above, breach response services will help to satisfy statutory responsibilities and protect the insured organization's reputation. Other valuable add-on services include
 - o Risk assessment of data/privacy exposures
 - o Risk control education for the organization's staff
 - o Client advisory bulletins on emerging exposures
 - o 24/7 claim hotlines
 - o Legal consultation by attorneys experienced in cyber risk

CONCLUSION

Data security breaches and identity theft are growing risks for health care organizations, due in part to their increased reliance on electronic medical records and electronic data storage. At the same time, an exponential increase in privacy laws has set the stage for more enforcement actions in more jurisdictions.

Traditional property and liability insurance policies were not designed to provide protection against these emerging risks. Coverage gaps in many traditional property & liability insurance policies range from data theft and destruction by hackers and liability for unauthorized disclosure of data by hackers to the cost of notifying patients whose confidential information has been compromised.

Cyber-insurance policies are designed to fill the coverage gaps left by traditional business insurance. However, these policies vary greatly with respect to coverage, limits, exclusions and definitions.

A few of the key differences among cyber-insurance policies include whether or not protection extends beyond an organization's Web site and online activities, whether or not there is coverage for claims resulting from a data security breach involving a third-party with custody of the insured's information, and whether or not full policy limit coverage is provided for legal defense of privacy regulatory proceedings and the costs of remediating a regulatory compliance deficiency. Cyber policies also differ greatly with respect to the services they provide to satisfy statutory responsibilities and protect the insured organization's reputation.

If a risk manager is uncertain about the adequacy of their coverage against privacy and data security risks, it is prudent to consult with a professional insurance advisor for a review of policies and coverages in order to identify potentially costly gaps in the organization's overall risk management and insurance program.

PRIVACY IN THE REGULATORY CROSSHAIRS

Healthcare providers are well aware of the mandates of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) as they relate to the security and privacy of protected health information. What they may NOT realize is the dramatic acceleration over the last five years of privacy rule enforcement by the United States Department of Health and Human Services (HHS) Office of Civil Rights.

Between 2003 and 2006, the number of HIPAA enforcement actions related to the security of personal health information increased sixfold - from 339 actions to 2,466.(4) In 2008, for the first time ever, HHS required a resolution agreement from a major healthcare provider, which resulted in a \$100,000 fine and an agreement to implement a detailed corrective action plan to address security issues surrounding electronic patient information.(5)

In addition, published reports from early 2008 indicate that HHS has contracted with the firm PricewaterhouseCoopers to conduct surprise audits of hospitals where complaints have been received about data security.(6) In some cases audits may be conducted at random even if there was no breach or complaint filed.(7)

Meanwhile, identity theft laws at the state level are proliferating with increasingly stringent notification requirements.(8) Some laws set a hard deadline for notification, e.g., Florida requires notice in 45 days of the breach and 10 days for third-party custodians of the data. Some laws, e.g., Texas and Wyoming, require notification even if the data was encrypted. Other laws, e.g., California, give affected parties a private right of action and imposes civil monetary penalties for patient safety deficiencies. If a healthcare organization treats patients from other states, the laws of the patient's home state also may apply. In addition, the 111th U.S. Congress will be seeking to strengthen HIPAA in this area.

Why do these issues raise critical concerns for healthcare risk managers? Because the defense of privacy regulatory actions is expensive, time-consuming and damaging to an organization's reputation. In short, regulatory pressure is one more reason to address identity and data security risk in an overall risk management and insurance program.

REFERENCES

1. "Identity Aftermath." September 23, 2003. Identity Theft Resource Center. www.privacyrights.org/ar/idthefts-surveys.htm#ITRC
2. "2005 Identity Fraud Survey Report." Jan. 26, 2005. Better Business Bureau and Javelin Strategy and Research. www.privacyrights.org/ar/idthefts-surveys.htm#BBB
3. "2007 Annual Study: Cost of a Data Breach." November 2007, p. 6., Ponemon Institute.
4. U.S. Department of Health and Human Services. www.hhs.gov/ocr/privacy/enforcement/numbers-glance0407.html.
5. U.S. Department of Health and Human Services news release, July 15, 2008. www.hhs.gov/ocr/privacy/enforcement/resolution.html.
6. NetworkWorld.com, 2/27/08, www.networkworld.com/news/2008/022708-healthcare-cyberattacks.html
7. "HIPAA Security Rule Enforcement: Prepare for an audit at your facility." Audio conference available for purchase at www.hcmarketplace.com/prod-6297.html
8. "Data Breach Notification Laws State by State." www.csoonline.com/article/221322/CSO_Disclosure_Series_Data_Breach_Notification_Laws_State_By_State

ABOUT THE AUTHOR

Mark Silvestri is the product manager for the CNA NetProtect® suite of information risk insurance products. CNA is a leading provider of insurance protection to healthcare organizations.

Any examples in this article are for illustrative purposes only and any similarity to actual individuals, entities, places or situations is unintentional and purely coincidental. This material is not intended to establish any standards of care, to serve as legal advice appropriate for any particular factual situations, or to provide an acknowledgement that any given factual situation is covered under any CNA insurance policy. Please remember that only the relevant insurance policy can provide the actual terms, coverages, amounts, conditions and exclusions for an insured. All products and services may not be available in all states and may be subject to change without notice. Any references to non-CNA Web sites are provided solely for convenience, and CNA disclaims any responsibility with respect to such Web sites. CNA is a service mark registered with the United States Patent and Trademark Office. Copyright © 2009 CNA. All rights reserved. Reprinted with permission.