HOSPITAL ASSOCIATION OF SOUTHERN CALIFORNIA®

February 19, 2015

Briefs Focus

Protect and Prepare Your Hospital for Cyber Attacks Through HASC's Cyber-Security Program

Scott Twomey

Mark Gamble

If you would like additional information about HASC's Cyber Security Program, please contact either Scott Twomey, Senior Vice President & CFO, HASC, at (213) 538-0756, stwomey@hasc.org, or Mark Gamble, Senior Vice President and Chief Operating Officer at HASC, at (213) 538-0760, mgamble@hasc.org.

Recent cyber-attacks at Anthem and Sony prove that cybercrime is a very real, evolving threat. Hospitals and health systems are attractive targets because cyber criminals can sell stolen electronic health care information on the black market for $50 per electronic health record (EHR). Even partial information from an EHR is much more profitable to the bad guys than stolen social security or credit card numbers, which garner just $1 per record.[1]

Stolen health care information is more valuable because it's used to file fraudulent insurance claims, obtain prescription medication and advance identity theft well beyond what can be achieved with a social security number.

In 2014, the FBI sent a notification to the health care industry stressing the need for improved cyber security[2]. The FBI stressed that health care organizations "are poorly protected and ill-equipped to handle cyber threats exposing patient medical records." The FBI also noted that EHR theft is more difficult to detect, taking almost twice as long to identify than the more common types of identity theft.

There is often a false sense of security that cyber liability is covered under a hospital's general liability (GL) policy. With the growing risk of cyberattacks, most insurance companies are excluding cyber risk from GL policies. And if there is coverage, it is bare bones. To respond to this growing, very real threat, HASC developed a comprehensive cyber-security program that provides hospitals with loss prevention services, insurance coverage and breach resolution services.

HASC's program was formed in conjunction with AmWINS, a wholesale insurance broker, hospital risk managers and IT representatives. Together, we identified AIG as the best-in-class insurance carrier in cyber-security and liability coverage.

Access to the program is available exclusively through HASC and AmWINS. Hospital insurance brokers should contact Dave Weller, Executive Vice President, AmWINS Insurance Brokerage of California, LLC, office: 213.254.2245, email: dave.weller@amwins.com.

The Cyber-Liability Insurance Program Summary

Participating hospitals benefit from the following services and coverage, all of which are included in the annual premium.

Risk Mitigation Services

• Infrastructure vulnerability scan by IBM.

• CyberEdge RiskTool specifically tailored to HASC members. RiskTool is powered by RiskAnalytics to deploy, manage and track network security and privacy training, for employees and independent contractors, information security processes/ procedures and business associate agreements.

Program Highlights

• AIG is "A" rated (Excellent) by AM BEST.

• Dedicated AIG underwriting team based in California.

• Coverage is written on "admitted paper" in California.

• 24/7 claim reporting capability.

• Designated Claim handling team exclusively for the HASC program.

• Two hours of legal consultation with AIG's partner law firm to review current information security policies and procedures.

• IP Shunning Technology powered by RiskAnalytics, as an extra layer of infrastructure technology service to a hospital's existing network security system.

• Access to 24/7 Technical Hotline supported by IBM to assist hospital IT personnel in diagnosing and responding to potential or actual security threats.

• Free access to AIG's CyberEdge Mobile App for iPhone®, iPad®, or Android™.

CyberEdge Cyber Liability Insurance Policy

Security and Privacy Event legal liability coverage – responds to important third-party liability for claims arising from:

• Failure of the insured's network security.

• Failure to protect personally identifiable information from misappropriation, including disclosures as a result of social engineering attacks (e.g., phishing).

• Failure to protect or wrongful disclosure of private or confidential information.

• Violation of any federal, state or local privacy statute alleged in connection with failure to protect private information.

Event Management Coverage – responds to the costs to retain public relations services to assist in managing and mitigating a covered privacy or network security incident.

• Event Management coverage can be purchased on a lump sum limit or an affected persons limit basis subject to premium differences.

• Includes costs to notify consumers of a release of private information. Such notification is now mandated by most states and can be very costly.

• Includes cost of credit-monitoring or other remediation services to help minimize damages to those victimized by a covered privacy or network security incident.

• Includes costs associated with losses to information assets such as customer databases resulting from a failure of network security.

• Provides vital protection for "intangible" assets that are not covered by traditional property insurance.

Network Business Interruption Coverage – responds to an insured's loss of income and operating expenses when business operations are interrupted or suspended due to a failure of network security.

• Broadened definition of loss includes lost business income, normal operation expenses (including payroll) and those costs that would not have been incurred but for the interruption.

Media Liability Coverage – Media Content Insurance addresses the liability faced by developing or distributing media content.

• Responds to claims arising out of all media distributed by the insured.

• Addresses claims arising from an insured's advertising materials.

• Provides protection for numerous perils, including trademark infringement; copyright infringement; defamation; false light; false imprisonment; product disparagement; infliction of emotional distress; failure to maintain the confidentiality of a source; and invasion of privacy.

• Responds to both online and off-line content.

Cyber Extortion – pays to settle network security or private information-related extortion demands made against the insured.

• Triggers when there is a threat to commit a computer attack against the insured or expose confidential information held by the insured and a demand for money to terminate the threat.

• Includes the costs of investigations to determine the cause of the security threat or privacy threat and to settle the extortion demand.

Coverage Enhancement Endorsements

• Provides automatic subsidiary acquisition for no additional premium at 15% of named insured revenues or less.

• 1st & 3rd party single retention if the event loss triggers more than one coverage section.

• Notice provision amended to include only non-administrative personnel.

• 60-day post-policy reporting provision.

• 60-day window to purchase extended reporting period beyond automatic 60-day extended reporting period.

- Policyholder choice of AIG panel counsel for defense representation.

• E-Discovery expense enhancement of $25,000 of the total policy limit for expenses incurred to comply with e-discovery requests.

• Criminal reward fund – up to $50,000 in addition to the limit of liability with no retention for a reward fund to be established for information leading to the arrest and conviction of persons responsible for illegal acts covered under the policy.

• Definition of "suit" expanded to include mediation.

• Prior knowledge exclusion limited to non-administrative personnel.

• Defense costs definition expanded to include reimbursement of insured lost earnings of up to $500 per day not to exceed $5,000 in connection with a covered suit.

• Criminal reward fund – up to $ 50,000 in addition to the limit of liability with no retention for a reward fund to be established for information leading to the arrest and conviction of persons responsible for illegal acts covered under the policy.

• Definition of "suit" expanded to include mediation.

• Prior knowledge definition limited to non-administrative personnel.

• Defense costs definition expanded to include reimbursement of insured lost earning of up to $500 per day not to exceed $5000 in connection with a covered suit. Coverage is part of and not in addition to the aggregate policy limit.

Exclusive HASC Coverage Enhancement Endorsement

• Definition of confidential information expanded to specifically include reference to California privacy statues.

• Expanded definition of loss in cyber extortion coverage to include costs for qualified consultation on how to respond to extortion threat.

• Definition of security failure expanded to include cyber terrorism.

• Event Management Coverage amended to provide zero retention for first response expenses incurred within the first 72 hours of discovery of a covered claim up to a maximum $50,000 provided the insured uses an AIG-preferred response vendor.

• Other insurance clause amended to list the cyber liability policy as primary over any hospital professional or medical malpractice policy.

• $25,000 Personal Identity Coverage for directors and officers, in addition to the limit of liability subject to zero retention for coverage of expenses related to a stolen identity event.

1. EMC2/RSA White Paper 2013
2. FBI Cyber Division, Private Industry Notification #:140408-009; April 8, 2014

This cyber liability insurance program is available exclusively through HASC. **As such, all retail insurance brokers in California can access the HASC program through AmWINS.**

For more information, hospital brokers should contact Dave Weller, Executive Vice President, AmWINS Insurance Brokerage of California, LLC, office: 213.254.2245, email: dave.weller@amwins.com.