Healthcare: The Financial Impact of a Data Breach
Healthcare Cyber Risks and Insurance Coverage Issues
Healthcare Cyber Risks: What is the Risk?

Background

As healthcare organizations become increasingly exposed to risks from data security breaches, and identity theft involving Protected Health Information (PHI) and/or Personally Identifiable Information (PII), it is worthwhile to explore what the risks to these organizations are and where they emanate from.

The advent and growth of our electronic networks has changed the risk profile for virtually every organization, but few have been more affected than healthcare organizations. In 1996, with the enactment of HIPAA, the subsequent involvement of the OCR, and the enactment of HITECH, have all made operating significantly lack the necessary capabilities to prevent, monitor and remedy a data breach event.

As these new risks continue to evolve and healthcare organizations continue to invest in technology infrastructure to streamline and manage their data, the depth and breadth of the potential costs and expenses as a result of a cyber data breach are still developing and not fully known. What is known is that healthcare organizations have already incurred significant costs and expenses from legal fees, notification costs, credit monitoring, fines, penalties and redress funds to address the outcome of unauthorized access to confidential patient information.

Within the healthcare space a compliance nightmare. 50 States have enacted either legislation or regulations mandating what must happen to notify residents in the event of a data breach involving their state. Data in every form, electronic and non-electronic is moving into, around and through the electronic ether. The security and safeguarding of information is paramount to protecting an organization from embarrassment, reputational damage, financial loss, regulatory intervention and even public boycotting.

Additionally, your patients demand that your organization protects their most intimate healthcare details, they trust that their information will remain private and secure regardless of where that information may reside, whether this is in a file cabinet at a doctor’s office, a chart being carried throughout a medical facility, or within a claim form at an insurance company. Your Information Technology (IT) department has been transformed, and is no longer a cost center, but rather an integral part of your organization. Most healthcare organizations have determined that the Chief Technology Officer/Chief Information Officer is a vital aspect of the organization and is involved in patient care from the moment the patient enters the door. Preservation of the integrity of the network and implementing an enterprise-wide privacy/security plan is a full time undertaking. IT requires intelligence, experience, unrelenting resources, robust budgets and vigilance. Unfortunately, many organizations

Increased Awareness

According to the 2015 Experian Data Breach Industry Forecast, data breaches in healthcare organizations are on the rise and will continue to be a target for cyber criminals due to the expanding number of access points to Protected Healthcare Information such as electronic medical records and wearable technology. The Third Annual Benchmark Study on Patient Privacy and Data Security by the Ponemon Institute cites 94 percent of all healthcare providers say they have had at least one data breach in the last two years. Most of these were due to employee mistakes and sloppiness, 46 percent of respondents in this study cite lost or stolen computing devices and 42 percent note unintentional employee action. Another disturbing cause is third-party error, including business associates, according to 42 percent of participants.
Additionally, widespread use of mobile devices is putting patient data at risk. 81 percent of healthcare organizations in this study report that they permit employees and medical staff to use their own mobile devices to connect to their organization’s networks or enterprise systems. However, 54 percent say they are not confident that these personally owned mobile devices are secure.

Boards of Directors and Stakeholders are beginning to fully recognize the catastrophic nature of cyber healthcare risks. Prudent risk management of cyber & technology healthcare risk should be one of the greatest concerns of any healthcare organization. This concern is exasperated greatly for publicly traded corporations and large privately held corporations that risk stakeholder litigation from mismanagement of cyber healthcare PHI.

The Financial Impact

Data breaches involving PHI can be damaging to the healthcare organization both financially and reputationally. According to the Ponemon Study cited above, it has been estimated that the average economic impact of a data breach is $2.4M. The major costs associated with the financial impact include credit monitoring, legal advice, defense, notification, public relations, forensics, data recovery and regulatory fines and penalties. These costs and expenses can be damaging and at times, overwhelming to an organization. Preparing for a data breach event must be considered. While the timing of such an event cannot be predicted, the fact remains, the question is not if the healthcare organization will have a data breach, it is when.

Mitigating these costs and the resulting financial impact to the healthcare organization can be addressed through the utilization of a cyber liability insurance policy and program. Outlined below are the types of insurance coverage that is currently available within the marketplace.

• **Network Security Liability** – provides liability coverage if an healthcare organization’s computer system fails to prevent a security breach or a privacy breach

• **Web Content Liability** – coverage for content-based injuries such as libel, slander, defamation, copyright, title, trademark infringement or invasion of privacy arising from the display of material on the healthcare organization’s website

• **Privacy Liability** – provides liability coverage if the healthcare organization fails to protect electronic or non-electronic information in their care, custody and control, or in the care, custody and control of an independent contractor.

• **Media Liability** – covers the healthcare organization for intellectual property and personal injury perils resulting from an error or omission in content (coverage for patent and trade secrets are generally not provided)

• **Regulatory Liability** – coverage for lawsuits or investigations by federal, state or foreign regulators relating to privacy laws

• **Notification Expense** – 1st party expenses to comply with privacy law notification requirements

• **Credit Monitoring Expense** – 1st party expenses to comply with privacy law credit monitoring requirements

• **Crisis Management** – 1st party expenses to hire a public relations firm

• **Data Recovery** – 1st party expenses to recover data damaged on an insured computer system as a result of a failure of security
• **Business Interruption** - 1st party expenses for lost income from an interruption to an insured computer system as a result of a failure of security

• **Cyber Extortion** – payments made to a party threatening to attack an insured’s computer system in order to avert a cyber attack

• **Professional Errors & Omission Liability** – miscellaneous E&O can be added to a policy when applicable.

How the healthcare organization responds to an event may be literally life or death. Understanding how the event occurred, what data has been breached, who was involved, where the data lies, how to effectively communicate with governmental entities and the public, and how to comply with the complexities and administrative burden of state and federal legislation, will be problematic for the smallest to the largest of entities.

Preparing for this type of an event and navigating this minefield will be crucial and critical to the survival of the organization. Having a strong partner at the onset of this event, which is available 24/7/365 is comforting. Many of the insurance solutions available in the insurance market today provide such a solution to their insureds. Pre-negotiated contracts with attorneys, notification companies, public relations firms and forensic firms are just a few of the services that will provide benefit and value to the organization as they move forward through the event.

What are some of the best practices that healthcare organizations can follow:

**PLAN, PREPARE, PRACTICE**

• Determine who is part of your Incident Response Team/Crisis Management Team

• Train staff to be familiar with privacy laws, rules and regulations

• Conduct event drills

**Know the rules**

• Privacy laws, regulations and guidelines

• Identify laws that are applicable to your organization

**Know your exposure**

• Where does the data exist?

• What data do we have?

• How long do we hold data for?

• Superfluous data should not be collected

• Internal/external third party reviews and audits are necessary

**Know your employees**

• Educate employees on what their role is and how they should handle data

• Conduct background checks
Know your entity’s network security risk
• Annual security risk assessments
• People/processes/technology

Know your business partners
• Third party vendors/independent contractors
• Inquire about their policies and procedures
• What does the indemnification language say, how are you protected?
• What is their responsibility to protect your data?

CONTAIN – the incident
RESPOND – based on findings from the investigation
RESTORE – confidence in the organization
RETAIN – patients

Manage Your Risk
The security and safeguarding of information is paramount to protecting an organization from financial loss, embarrassment, reputational damage and regulatory intervention. The depth and breadth of the potential costs and expenses from a breach of a social network are still developing, dynamic and not fully known.

The following are some known cyber risk exposures of the healthcare industry:
• Errors, omissions and negligent acts in the performance of services online and offline
• HIPAA violations
• Privacy breaches, including identity theft
• Unauthorized access
• Debilitating viruses
• Federal governance and compliance
• Libel, slander and defamation
• Copyright, title and trademark infringement
• Destruction, corruption or theft of bandwidth
• Cyber extortion threat
• Malicious breaches of security by internal users

What are underwriter concerns when looking to provide adequate coverage for a Healthcare Organizations?
Here are some common questions underwriters will ask:
• Is Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII) encrypted when e-mailed?
• Is PHI and/or PII encrypted on the server and mobile devices?
• Do security features provide degrees of access control to physicians?
• What type of institution detection will be deployed and how often is the system checked for updates to software?
• How many records does your entity have in electronic or paper format?
• On the entity’s website or portal, will there be a chat room, and will blogs allow comment and discussion? What are the screening and take down procedures for content (including music and videos)?
• What type of third party content will be made available on the portal, and will counsel review content before it is posted? Will the portal provide medical advice? Who has access to that medical advice?