Healthcare
Cyber Risk and Solutions

Cyber risk has become a leading issue for many organizations as awareness of cloud computing, social media, corporate Bring Your Own Device policies, big data, and state-sponsored espionage has grown and recently been amplified by President Obama's Cybersecurity Executive Order. In an increasingly punitive legal and regulatory environment, and in the face of more frequent contractual insurance requirements specifying cyber liability, forward-thinking companies are taking proactive steps to explore and transfer cyber risk.

When should organizations be concerned about their cyber risk exposure?

Organizations should be concerned about cyber risk if they:

- Gather, maintain, disseminate or store private information
- Have a high degree of dependency on electronic processes or computer networks
- Engage vendors, independent contractors or additional service providers
- Are subject to regulatory statutes
- Are required to comply with PCI Security Standards/Plastic Card Security statutes
- Are concerned about contingent bodily injury and property damage that may result from cyber incidents
- Rely on or operate critical infrastructure (Personally Identifiable Information risk are less prominent for industries such as utilities, manufacturing and logistics)
- Are concerned about intentional acts by rogue employees
- Are a public company subject to the SEC Cyber Disclosure Guidance of 2011

What are unique risks to healthcare clients?

- Subject to regulatory statutes such as the Health Insurance Portability & Accountability Act (HIPAA) and the Health Information Technology for Economics & Clinical Health Act (HITECH); adds an element of liability created by Business Associates, vendors and other service provider
- Extensive amounts of Personally Identifiable Information (PII) and Protected Health Information (PHI) transmitted and stored on system
- Mobile and tablet computing in offices/hospitals
- Heavy dependencies on outsourced service providers such as payment processors and laboratory test processing partially due to budgetary pressures
- Complex chain of liability from providers, payors, third party administrators, technology or hardware firms, pharmacy benefit managers, outsourced network service providers and data storage firms
- Many users leaving door open to human error
- Network systems typically allow multiple points of access (including outsourced vendors)
- Creation and implementation of Electronic Health Records (EHRs) and Personal Health Records (PHRs)
- Sharing of health information with a variety of providers, including specialists

Why are standard insurance policies not enough?

While existing forms sometimes carry a level of coverage, they were not intended to cover many risks associated with an increasingly digital world. Typical forms respond as follows:

- **General Liability:** covers bodily injury and property damage, not economic loss
- **Errors & Omissions:** covers economic damages resulting from a failure of defined services only, and may contain exclusions for data and privacy breaches

We're here to empower results

Christian Hoffman
christian.hoffman@aon.com
+1.212.441.2263

Brent Rieth
brent.rieth@aon.com
+1.415.486.7162

Eric Seyfried
eric.seyfried@aon.com
+1.212.441.1406

John Brosnan
john.brosnan@aon.com
+1.312.381.4562

Stephanie Dingman
stephanie.dingman@aon.com
+1.312.381.5146

Stephanie Snyder Tomlinson
stephanie.tomlinson@aon.com
+1.312.381.5078

aon.com

- **Property Insurance:** covers tangible property, which data is not. Loss must be caused by a physical peril while perils to data are viruses and hackers
- **Crime:** covers employees and generally only money, securities and tangible property. No coverage for third party property such as customer/client data

What is the scope of today's cyber coverage?

3rd Party Coverage

- Wrongful disclosure of Personally Identifiable Information, Protected Health Information or confidential corporate information in the client's care, custody or control via a computer network or off-line (e.g., via laptop, paper, records, disks)
- Failure of computer network security to guard against threats such as hackers, viruses, worms, Trojan horses and denial of service attacks whether or not resulting from the provision of professional services
- Content liability perils such as defamation and infringement of intellectual property rights arising out of website, marketing and advertising activities
- Security or privacy breach regulatory proceedings (including associated fines and penalties)

1st Party Coverage

- Network business interruption: loss of income and extra expense due to network security failure
- Intangible property: costs to restore or recreate data or software resulting from network security failure
- Breach response/management costs associated with:
  - Breach notification, including the hiring of outside law firms and public relations consultants
  - Credit monitoring/protection
  - Notification hot-line/call center
  - Forensic costs
  - Identity theft resources
- Cyber extortion
- Loss of income due to failure of network security

How do organizations transfer cyber risk?

- Some exposures can be transferred contractually if outsourcing services. Insurance solutions exist if vendor will not take responsibility
- Marketplace evolving to provide services solution, including loss control resources, data breach coaches, dedicated claims resources, pre-approved panels of vendors and service providers to address each element of breach response
- Many insurers provide cyber coverage on a primary basis
  - Breach response coverage offering varies based on insurer and policy structure
- Numerous additional insurers available for consideration of excess limits

Aon Approach

- **Strategic Meetings / Discussions** – Aon takes a collaborative approach with our clients to identify and analyze exposures, risk and potential insurance including proposed structures, or alternative solutions
- **Submission Development** – Aon works with our clients to obtain relevant, necessary and favorable underwriting information to present to markets
- **Marketplace Leverage** – Aon puts our vast knowledge of market conditions and trends to work on behalf of each client, negotiating favorable terms and conditions with top tier carriers
- **Strategic Negotiations and Placement** – Aon utilizes proven and sophisticated negotiation strategies to finalize placements that meet collaboratively established goals

Throughout the process Aon advises on Cyber risk management best practices and provides frequent thought leadership and guidance on emerging exposures and coverage issues.