Dallas Bar Association Health Law/
Tort & Insurance Practice Sections

April 25, 2018

Cyber Liability Insurance: Understanding What Is & Isn't Covered

John Southrey, CIC, CRM
Texas Medical Liability Trust (TMLT)
Director of Consulting Services

Cyber Risk Self-Assessment

YES	NO	
		Do you use any computing devices that leave your office such as laptops, PDAs, smart phones, mobile interface devices of any kind?
		If you store any data on mobile devices or if the devices can be used to access your network, are all mobile devices encrypted?
		Do you gather or store any data on a physical medium, such as paper?
		Do you provide data to any third party for storage or to perform a process or business function with it? Does any third party have access to your data or systems either electronically or physically?
		Do you provide technology or telecommunication services to others for a fee?
		Do you have a Facebook, Twitter, or other social media account?
		Do any of your employees post on social media platforms?
		Do you have a website? If so, do you gather data on it or provide any services through it?
		Are you dependent upon the Internet or your computer system to generate revenue?
		Do you accept credit/debit cards for payment of goods or services (even if you never store or process the data)?

If you answered "YES" to any of these questions, a data breach could result in a first-party and/or third-party financial loss to your organization.

What's Your Cyber Cost of Risk?

"… the true risk, cost and prevalence of cyber-attacks in healthcare is likely far greater than most are aware. Chronic under-investment in cybersecurity has left many so exposed that they are unable to even detect cyber-attacks when they occur."

The Rampant Growth of Cybercrime in Healthcare, Feb. 08, 2017. Workgroup for Electronic Data Interchange (WEDI)

What's Your Cyber Cost of Risk? (cont.)

"If you don't know your [cyber] risks, you're extraordinary vulnerable — and the financial costs of a data breach can be staggering."

Mary Chaput, CFO, Clearwater Compliance

(Cybersecurity is really about mitigating the direct and indirect costs of a data breach.)

"A Failure In Imagination" [post 9/11]

Businesses often underestimate the probability, prevalence, and severity of cyber attacks.

The actual costs for remediation and for damages can be significantly higher than anticipated at the time of loss or what is likely reported.

The Potential Economic Impact

Economic Impacts on an Organization in Health Care and Across All Industries

	Health Care Organization[1]	Across All Industries[2]
Detection and Escalation	$30,000 to $1.6M	$1,250 to $4.9M
Notification	$4,000 to $1.7M	$14M to $15M
Follow-up response (legal, public relations, credit monitoring)	$60,000 to $5.8M	$5,000 to $3M

Cyber Security: Law and Disorder Understanding New Challenges in Cyber Security and How Provider Organizations Can Prepare.
Advisory Board 2017; Health Care IT Advisor

An Actual TMLT Policyholder Claim

Jan. 22, 2017 – Ransomware Attack
- 279,663 Patients Notified
- $630,000 Initial Claim Reserve
- $100,000 TMLT Cyber Liability Triggered

Mar. 22, 2017 – OCR is Notified
- OCR Initiates Investigation
- OCR's Data Request Requires Completion

May 26, 2017 – Primary Limits Exhausted
- $1M "Buy-Up" Cyber Liability is Triggered
- Current Claim Reserve is $710,000
- $100K + $471K ($571K) Paid-To-Date
- OCR Investigation is Ongoing

"Dear Mr. Southrey, …

Our investigation indicates that your personal information may have been impacted by ransomware, including your name, address, date of birth, Social Security number, and medical information.

… we have taken steps to prevent a similar event from occurring in the future, *including improving our network security, updating our system back ups,* and *retraining our employees* regarding suspicious emails and patient privacy …."

Cybersecurity Is An Enterprise Risk!

- IT staff/Entire Workforce
- EHR Software Vendors*
- Managed Service Providers*
- Cloud Service Providers*

*You can't totally accept what vendors/BAs tout about their data security or their "HIPAA compliance." And "moving to the cloud" (even with enterprise-grade security) doesn't completely shift the breach risk.

Cloud-based Systemic Risk

"Cloud computing has its own inherent vulnerabilities, which can create common risks among end users. …. it can be assumed that all systems being hosted on the network will in turn be vulnerable to exploitation [and cloud downtime].

This leads to a great degree of *risk correlation* between firms from cyber threats that otherwise would not exist if the firms' data and services were located locally."

The Cost of Malicious Cyber Activity to the U.S. Economy, The Council of Economic Advisers, February 2018

After a Breach: Who Is Responsible?

- Who owns the data?
- Who will notify the affected individuals, local media, and regulatory authorities?
- Who pays for the notifications and press releases?
- Who pays for the forensics to determine the causation of the breach and if any personal data was exfiltrated?
- Who pays for the credit monitoring and identity theft restoration services for the affected individuals?
- Who will indemnify whom?
- Do the contracting parties have cyber insurance that covers *liability assumed under contract?*

Direct & Indirect Costs of a Breach

Direct Costs:

- Legal Fees
- IT Forensics
- Data Restoration
- Notifications & Credit Monitoring
- Public Relations & Media Release
- Call Center Support
- Regulatory Fines & Penalties
- Third-Party Damages
- IT Upgrades/Fixes

Indirect & Opportunity Costs:

- Business Disruption/Interruption
- Patient Churn & Reputational Harm

Role of Cyber Liability Insurance

In March 2015, at a U.S. Senate hearing on Cyber Insurance it was noted:

"Simply engaging in the process of seeking cyber insurance coverage can assist businesses to develop the correct approach to mitigate risk. Insurance can bring all relevant stakeholders in an organization together, encouraging an enterprise-wide risk management approach."

http://www.propertycasualty360.com/2015/03/20/cyber-insurance-in-the-spotlight-senate-mulling-fe

Role of Cyber Liability Insurance (cont.)

"I think the cyber insurance industry has enormous potential to positively shape the cybersecurity ecosystem in this country. …

If I was an insurance company and I was underwriting a company, I would not underwrite them unless I knew every day how secure they were."

Richard C. Clarke, former National Coordinator for Security, Infrastructure Protection and Counter-Terrorism for the U.S.
www.insurancejournal.com/news/national/2017/11/15/471130.htm

Role of Cyber Liability Insurance (cont.)

"As the cyber threat increases so too does the demand for cyber insurance.

… insurers' understanding of cyber liability and risk aggregation is an evolving process as their experience of cyber-attacks increases. …

This report's findings suggest economic losses from cyber-events have the potential to be as large as those caused by major hurricanes."

Counting the cost – cyber exposure decoded.
Emerging Risks Report 2017 Technology, Lloyd's

What Is Cyber Insurance?

Cyber Insurance covers confidential consumer, corporate, and employee information. It pays for media, privacy, and security *wrongful acts* resulting in claims from third parties and employees; and for cyber extortion; hacking and virus attacks; regulatory fines and penalties; and breach response services.

Cyber policies are either claims-made or occurrence based and there is no form standardization. Most policies will include both first-party coverage agreements and third-party coverage agreements.

First-Party & Third-Party Coverages

First-Party (Insured's Loss):

- Breach Response Costs
- Network Asset Protection (incl. Business Interruption)
- Cyber Extortion & Cyber Terrorism
- Cyber Crime
- Brand/Reputation Loss

Third-Party (Insured's Legal Liability to Others):

- Multimedia Liability
- Security & Privacy Liability
- Privacy Regulatory Defense and Fines & Penalties
- Payment Card Industry DSS Liability/Assessments
- Technology Errors & Omissions

Emerging Cyber Coverages

OCR Corrective Action Plan Costs
- Expenses to complete a security risk assessment and to complete a HIPAA compliance audit

Post-Breach Remediation Costs
- Expenses to conduct a security gap analysis and security awareness training

Third-Party Breach Notification Costs
- Expenses to notify affected individuals for a third-party

Contingent Bodily Injury & Property Damage
- Expenses to pay third-party damages arising from bodily injury and/or property damage

Dependent/Contingent Business Interruption
- Expenses to pay the loss of net income and extra expenses, if a third-party service provider's network goes down

Cyber Liability Coverage Example

Named Insured(s):

	Multimedia Liability:	$2,000,000
	Security and Privacy Liability:	$2,000,000
	Privacy Regulatory Defense & Penalties:	$2,000,000
★	Breach Event Costs (*Outside Limits*):	$2,000,000
	Network Asset Protection:	$2,000,000
	Cyber Extortion:	$2,000,000
	Cyber Crime:	$100,000
	PCI DSS Liability:	$1,000,000
	Maximum Policy Aggregate:	$2,000,000
	Retentions:	$5,000

Retentions can also be the no. of affected individuals or a time-based "waiting period" (e.g., 8 hrs.)

❖ *Breach Event Costs* are outside the maximum policy aggregate limit of liability. Therefore, these expenses will not reduce and are in addition to the maximum policy aggregate limit—providing a potential maximum policy aggregate of **$4,000,000**.

Who Is Insured?

- The **Named Insured** and any **Subsidiary**;
- Any **officer**, **director**, **trustee** or **employee**;
- Any **agent** or **independent contractor**, *but only while acting on behalf of the Named Insured*;
- Any **person** or **legal entity** the Named Insured *is required by written contract* to provide such coverage (e.g., as an Additional Insured or Indemnitee).*

**Liability assumed under contract* is covered for third-party damages, where such liability has been assumed in a written hold-harmless or indemnity agreement.

Contract Insurance Requirements?

"The following are contractual insurance requirements that XYZ hospital wants our organization to maintain:

- ✓ **Computer Processor/Computer Consultant Professional Liability Insurance** with a minimum amount of $3 million per claim and $5 million aggregate;
- ✓ **Privacy and Network Security Insurance** covering loss or disclosure of confidential information in a minimum amount of $5 million per loss; and
- ✓ **Third Party Fidelity/Crime Coverage**, including **Blanket Employee Dishonesty** and **Computer Fraud Insurance**, for fraudulent or dishonest acts committed in a minimum amount of $1 million per loss;

Plus naming the hospital as an **Additional Insured** on a *primary & non-contributory basis* with **Waiver of Subrogation**."

Two Key Coverage Definitions

Privacy breach means a breach committed by an Insured or by others acting on behalf of, for whom the Insured is legally responsible, including service providers.

Security breach means unauthorized access to or unauthorized use or infection of the "Insured's Computer System**."**

In Other Words …

- Coverage for data breach claims arising from the acts of any persons for which the Named Insured may be held responsible, including employees, independent contractors, and service providers.
- Coverage for **Insured's Computer System** includes a system operated or owned by the Named Insured or by a Service Provider, if the latter provides hosted computer application services or processes or stores the Insured's electronic data.*

*[Note: Avoid definitions that limit coverage to computer systems **only under the Insured's direct operational control**.]

Cybercriminals Hottest Schemes

Cyber Extortion (e.g., Ransomware)
Covers the extortion expenses and payment of extortion monies, subject to the insurer's consent, to respond to a cyber extortion threat or demand.

Cyber Crime (e.g., email fraud scams)
Covers *financial fraud loss*, *telecommunications fraud loss*, and *phishing attack loss* (including third-party loss) arising from cyber crime.

Clinical Risk From Ransomware

"It won't be long before a patient brings a private lawsuit against a healthcare institution for damages caused by the institution's *negligent security practices*, which led predictably to a loss of data access and thereby to a bad clinical outcome … [because of an] inability to function as expected due to a ransomware attack."

David Harlow with The Harlow Group

Key Coverage Pitfalls & Obligations

- Bodily Injury and/or Property Damage exclusion
- Cyber extortion exclusion
- Unencrypted data stored on mobile devices exclusion
- Infringement of Intellectual Property exclusion or Media Liability limited to website or social media activity only
- Failure to maintain security of IT systems with industry standards, best practices, or regulations exclusion **!**
- Liability assumed under contract exclusion
- Limited "Who Is Insured" definition
- Look for "sub-limited" coverage(s)
- Obligation to timely report a claim (e.g., within 30-60 days)
- Obligation to be truthful about cybersecurity posture

The Claim Process

Report the claim to your cyber insurer's claims department!

- "Breach coach" will be assigned and will likely hire a:
  - Panel Attorney
  - Forensic Expert
  - Notification & Credit Monitoring Co.
  - Public Relations Firm
- The insurer will typically not pay for services obtained without its prior authorization.
- Report the incident to your local FBI office.
- Also report the incident to your D&O; E&O; Commercial Crime; and Property & Casualty insurer for any "concurrent coverage."

Final Insurance Guidance …

Find a knowledgeable cyber insurance agent/ broker to help your client navigate the application process and to determine:

- What is the scope of coverage (i.e., what is & isn't a "covered loss" and what makes a "claim")?
- What limits of liability and coverage options does the client need?
- How the client might calculate the cost of data breach (i.e., the costing methodology to use)?

Providers Need External Experts' Help

As the forms of connected technologies/IoT devices used in healthcare increases — so will the cyber risks!

Therefore; healthcare providers will need assistance in mitigating the proliferation and diversity of their cyber vulnerabilities, including help with:

- ✓ **Risk Assessments**;
- ✓ Hardening IT systems;
- ✓ Vulnerability & Penetration Testing;
- ✓ Developing Policies & Procedures;
- ✓ Workforce Data Security Training;
- ✓ Incident Response Planning; and
- ✓ Cyber Insurance

Cybersecurity: A Social Good

"Cybersecurity is a common good. Thus, weak cybersecurity carries a cost not only to the firm itself, but also to the broader economy through *negative externalities* [i.e., spillover effects] imposed on the firm's customers and employees and on its corporate partners."

The Cost of Malicious Cyber Activity to the U.S. Economy, The Council of Economic Advisers, February 2018

Contact Info:

John Southrey, CIC, CRM
Director of Consulting Services
john-southrey@tmlt.org

Texas Medical Liability Trust
P.O. Box 160140
Austin, TX 78716-0140
ph: (800) 580-8658
direct: 512-425-5976
www.tmlt.org