HCCA Dallas Regional Conference

February 16, 2018

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

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

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 underinvestment 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)

Cyber Threats Can Be A Huge Risk

"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.)

Cybersecurity Is An Enterprise Risk!

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

*You can't totally accept what your vendors/BAs hype about their data security or their "HIPAA compliance." And "moving to the cloud" doesn't completely shift the risk. **It's your customer data**, **so you remain responsible for its security**.

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 …."

After a Breach: Who Is Responsible?

- 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 any *liability assumed under contract?*

A Word About Contractual Obligations

- Do you know if liability coverage comports with your contractual obligations?
- Liability insurance can be a financing mechanism for contractual indemnification or can act as a financial backstop when indemnification fails.
- Having the proper liability coverage can enable you to sign contracts with other parties who require contractual indemnification.*

*An *Indemnity Agreement* is not insurance.

Direct & Indirect Costs of a Breach

Direct Costs:
- Legal
- IT Forensics
- Data Restoration
- Notifications & Credit Monitoring
- Public Relations & Media Release
- Call Center Support
- Regulatory Fines & Penalties (OCR; TX AG; TMB)
- Third-Party Damages

Indirect Costs:
- Business Interruption: Lost Productivity, Loss of Net Income and Extra Expenses
- Diminished Patient Goodwill & Reputation Loss

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

What Is Cyber Liability Insurance?

Cyber insurance is a distinct insurance policy that provides both *first-party* coverage for intangible property losses and *third-party* coverage for related liability losses.

The coverage forms are not standardized. And as the threats have evolved, so have the policy forms.

- What is the scope of coverage; what is & isn't a "covered loss"?
- What limits of liability does your business need?
- How do you calculate your cyber exposure to loss? (e.g., use "breach calculators")

First-Party & Third-Party Coverages

First-Party Coverages (For Your Loss):

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

Third-Party Coverages (For Your Legal Liability to Others):

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

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

- *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**.

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 interruption expenses, if the system of an IT service provider goes down

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 (e.g., Service Level Agreements).

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 "Named 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. Covers the data stored by the Named Insured and by its vendors.
- Coverage for **Named 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.

Cybercriminals Latest Schemes

Cyber Extortion (aka "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
Covers *financial fraud loss*, *telecommunications fraud loss*, and *phishing attack loss* (including for a third-party) arising from cyber crime.

Clinical Risks From Cyber Attacks

"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

✶Plus the clinical risks that could arise from hacked medical devices!

Key Coverage & Obligation Pitfalls

- Bodily Injury and/or Property Damage excluded
- Criminal Acts excluded (except for innocent Insureds)
- Cyber extortion excluded
- Unencrypted data stored on mobile devices excluded
- "Sub-limited" coverage(s)
- Infringement of Intellectual Property excluded
- Failure to maintain the security of IT systems with industry standards, best practices or regulations **(!)**
- Costs to repair or update computer hardware excluded
- Liability assumed under contract excluded
- Obligation to timely report a cyber claim (30-60 days)
- Obligation to be truthful about network data security

The Claim Process

Report the claim to cyber insurer's claims department!

- A "breach coach" will be assigned who will then hire expert service vendors, including perhaps a:
  - Privacy attorney
  - Forensic expert
  - Notification & Credit Monitoring Co.
  - Public Relations Firm
- The insurer may not pay for services obtained without its prior authorization.
- Also report the incident to your local FBI office.

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:

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

Final Insurance Guidance …

- An underwriter typically uses a combination of *business risk class*, *record count*, and/or *revenue* to determine the premium.
- Find an knowledgeable cyber insurance agent/broker to help you navigate the application process and to determine the coverage options you may need.
- The agent should address the importance of having both robust cyber risk management (it's primary) and cyber liability coverage.

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 ext. 5976
direct: 512-425-5976 | cell: 512-589-4543
www.tmlt.org