Introduction to Cyber Risk & Insurance

Prepared for the Construction Financial Management Association

Date: August 18, 2016
Agenda

1. An Overview of Cyber Risk Exposures
2. Legal & Regulatory Trends
3. Marsh’s Cyber Risk Management Framework
4. Cyber Insurance Coverages
5. Cyber Risk Management Best Practices
Cyber Attacks – A Growing Global Risk

- Costs businesses $400B+ per year
- The world is becoming more dependent on the internet – an estimated 50 billion connected devices in the world by 2020 – 6.5 devices for every person on the planet.

Source: Marsh & McLennan Companies CYBER RISK HANDBOOK 2015
**Broader Exposures & Threats**

- Liability to Customers, Key Vendors and Employees
- Operational Disruptions
- Regulatory Scrutiny
- Notification Requirements
- Reputation

---

**CYBER BY THE NUMBERS**

<table>
<thead>
<tr>
<th>Market Overview</th>
<th>Cost of Cyber</th>
</tr>
</thead>
</table>
| **$446 billion** | **$5.9 million**
| **$120 billion** | **40%**
| Expected size of the global cyber security market in 2017. | Percentage of breaches that exceed $500,000 in losses. |
| **40 million** | **$1.8 million**
| Number of people in the US who had their personal information stolen by hackers in 2014. | Average post-breach costs. |
|                | **$3.3 million**
|                 | Average lost business costs. |
An Evolving & Headlining Risk

Headline News

Target Hacked: Retailer Confirms Unauthorized Access of Credit Card Data


Extramarital Affair Website Ashley Madison Has Been Hacked


Ransomware Wreaking Havoc in American & Canadian Hospitals


21.5 Million Exposed in Second Hack of Federal Office

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus non odio non ligula aliquet eu at velit. Donec in viverra libero.

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus non odio non ligula aliquet eu at velit. Donec in viverra libero.

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus non odio non ligula aliquet eu at velit. Donec in viverra libero.

WHY IT MATTERS?

- Value of Personal Data
- Cost of Cyber Breach ($5.9M average)
- Enterprise-Wide Risk Issue
- Difficulty Quantifying the Risk
- Frequency and Severity of Losses Seen
- Regulatory concerns
Recent Cyber Breaches in Construction

1. Turner Construction (2016)

   • Spear-phishing scam targeting 41 companies
   • Employee sent tax information on current and past employees to a fraudulent email account
   • Information included the full name, social security number, state of residency and tax withholding amounts.

2. Whiting-Turner Contracting (2016)

   • Vendor hired to perform tax services for Whiting-Turner
   • Whiting-Turner experienced suspicious activity on their systems and some employees reported fraudulent tax filings in their names
   • Vendor’s access was shut down and the investigation is ongoing
   • Potentially exposed information includes names, dates of birth, social security numbers and the names of any minor dependents.
There are Many Types of Cyber-Vulnerable Assets

- Technology Infrastructure
- Corporate IP
- Third-Party Data
- Brand & Reputation
- Financial Assets
- Cyber-Exposed Physical Assets
The Threat Environment

**Technology**
- Viruses, SQL Injections, DDoS attacks, etc.
- Social Media/Networking
- Phishing

**External**
- Vendors/Suppliers (contractors, outside counsel, cloud providers)
- Foreign and domestic organized crime
- Hackers/Hacktivists

**Internal**
- Rogue employees
- Careless staff
- BYOD

**Old School**
- Laptop theft
- Dumpster diving
- Photocopier

**Regulatory**
- DHHS - HIPAA
- SEC, FTC, state attorney generals
- 47 State breach notification laws (NM proposed)
- PCI Compliance
Types of Data Breaches: 2006 - 2015

Source: Verizon Data breach report 2016
The Uncontrollable Human Element

Vector of malware installation

- E-MAIL ATTACHMENT: 39.9%
- E-MAIL LINK: 37.4%
- WEB DRIVE-BY: 16.6%
- DIRECT INSTALL: 3.6%
- DOWNLOAD BY MALWARE: 2.8%
- WEB DOWNLOAD: 2.2%
- REMOTE INJECTION: 1.9%
- NETWORK PROPAGATION: 0.3%

Source: Verizon Data breach report 2015
The Reality...

In this corner, we have firewalls, encryption, antivirus software, etc.
And in this corner, we have Dave!!
Cyber Litigation Overview

Cyber litigation falls into 3 areas:

1. **State Enforcement Actions**
   - The state alleges a failure to provide adequate security for personal information and/or a failure to provide timely notification to affected individuals or the AG’s office
   - 47 state breach notification laws, with similar but differing requirements

2. **Federal Trade Commission Enforcement Actions**
   - FTC Act prohibits “unfair or deceptive acts or practices in or affecting commerce”
   - Over 50 settlements with companies over the failure to protect personal information of consumers
   - Wyndham hotels case affirmed FTC’s ability to regulate

3. **Civil Suits**
   - Cause of actions include negligence, breach of contract, unfair/deceptive trade practices and violations of privacy/cyber security statutes
   - Key issue = whether plaintiffs have standing to sue
Civil Suits – Surviving the Motion to Dismiss

Courts are now approving class actions relating to cyber breaches brought by:

**Consumers**
- Previously the Supreme Court held that the likelihood of injury to consumers arising from cyber breach is not sufficient to bring a class action\(^1\)
- Cases of *Adobe*\(^2\) and *Neiman Marcus* \(^3\) found that likelihood of injury was sufficient and allowed class action to proceed

**Employees**
- Case of *Sony*\(^4\) allowed class action brought by employees affected by data breach to proceed

**Financial institutions**
- In September 2015\(^5\) banks affected by the Target cyber breach were allowed to proceed with a class action

---

1. *Clapper v Amnesty International* 133 S. Ct. at 1147
Regulatory Trends to Watch…

Securities Exchange Commission ("SEC")

- Conducting investigations of public companies regarding:
  - Adequate disclosure of cyber risks
  - Proper internal controls to prevent breach
  - Proper disclosure to market following cyber breach

- Target investigated following breaches – no prosecution but significant expenses in responding to investigations

- SEC Guidance notes released in April 2015 and September 2015 aimed at investment industry. Highly likely that further guidance will be released relating to other industries
A thorough understanding of your risk profile is critical for cyber risk management, and that means more than just the typical compliance audit. You need to inventory your cyber-vulnerable assets, identify new and emerging threats, and model the potential impact of an event. And given the dynamic and ever-evolving nature of the risk, you must have the discipline to continuously gauge changes in your risk profile – and adapt.

Cyber risk management requires a balanced approach of:

**Prevention** — to stop cyber-attacks from succeeding.

**Preparation** — to make sure you are ready when an event happens.

**Risk Transfer** — to transfer cyber risk off your balance sheet.

You can’t eliminate cyber-attacks, but you can control how you handle them, and the decisions you make after an event make a big difference. When a threat, breach, or attack occurs, you need to detect it as soon as possible and react quickly. A quick, effective response and clear communication with internal and external stakeholders is essential.
Understanding the Gaps in Coverage

TYPES OF POLICIES

- GENERAL LIABILITY
- PROPERTY
- D&O
- ERRORS AND OMISSIONS
- FIDELITY AND CRIME
## Sample Gap Analysis

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Indemnification of your notification costs, including credit monitoring services</td>
<td>Not Covered</td>
<td>Not Covered</td>
<td>Not Covered</td>
<td>Not Covered</td>
<td>Not Covered</td>
<td>Not Covered</td>
<td>Privacy Liability</td>
</tr>
<tr>
<td>Defense of regulatory action due to a breach of privacy regulation</td>
<td>Not Covered</td>
<td>Not Covered</td>
<td>Not Covered</td>
<td>Not Covered</td>
<td>Not Covered</td>
<td>Not Covered</td>
<td>Privacy Liability</td>
</tr>
<tr>
<td>Coverage for fines and penalties due to a breach of privacy regulation</td>
<td>Not Covered</td>
<td>Not Covered</td>
<td>Not Covered</td>
<td>Not Covered</td>
<td>Not Covered</td>
<td>Not Covered</td>
<td>Privacy Liability</td>
</tr>
<tr>
<td>Threats or extortion relating to release of confidential information or breach of computer security</td>
<td>Not Covered</td>
<td>Not Covered</td>
<td>Not Covered</td>
<td>Not Covered</td>
<td>Not Covered</td>
<td>Covered</td>
<td>Cyber Extortion</td>
</tr>
<tr>
<td>Liability from disclosure of confidential commercial and / or personal information (i.e. breach of privacy)</td>
<td>Not Covered</td>
<td>Not Covered</td>
<td>Not Covered</td>
<td>Not Covered</td>
<td>Not Covered</td>
<td>Covered</td>
<td>Privacy Liability</td>
</tr>
<tr>
<td>Liability for economic harm suffered by others from a failure of your computer or network security (including written policies &amp; procedures designed to prevent such occurrences)</td>
<td>Not Covered</td>
<td>Not Covered</td>
<td>Not Covered</td>
<td>Covered</td>
<td>Covered</td>
<td>Covered</td>
<td>Security Liability</td>
</tr>
<tr>
<td>Website infringes on IP or is defamatory</td>
<td>Not Covered</td>
<td>Not Covered</td>
<td>Not Covered</td>
<td>Not Covered</td>
<td>Not Covered</td>
<td>Covered</td>
<td>Media Liability</td>
</tr>
<tr>
<td>Destruction, corruption or theft of your electronic information assets / data due to failure of computer or network</td>
<td>Not Covered</td>
<td>Not Covered</td>
<td>Covered</td>
<td>Covered</td>
<td>Covered</td>
<td>Covered</td>
<td>Data Property</td>
</tr>
<tr>
<td>Theft of your computer systems resources</td>
<td>Not Covered</td>
<td>Not Covered</td>
<td>Covered</td>
<td>Covered</td>
<td>Covered</td>
<td>Covered</td>
<td>Data Restoration</td>
</tr>
<tr>
<td>Loss of revenue and extra expense incurred due to a failure of security</td>
<td>Not Covered</td>
<td>Not Covered</td>
<td>Covered</td>
<td>Covered</td>
<td>Covered</td>
<td>Covered</td>
<td>Business Interruption</td>
</tr>
</tbody>
</table>
In the above chart, “growth rate” refers to the percentage increase from first half of 2014 to first half of 2015 in the number of clients purchasing standalone cyber insurance. “Take-up rate” refers to the overall percentage of clients that purchased standalone cyber insurance.
## Cyber Insurance Overview – First Party Coverage

<table>
<thead>
<tr>
<th>Coverage</th>
<th>Description</th>
<th>Covered Costs</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1st Party Insurance coverage:</strong></td>
<td><strong>Business Income/ Extra Expense</strong></td>
<td>• Loss of Income.</td>
</tr>
<tr>
<td></td>
<td>Interruption or suspension of computer systems due to a network security breach. Coverage may be limited to security attacks or broadened to include general system failure.</td>
<td>• Costs in excess of normal operating expenses required to restore systems.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Forensic expenses to value a loss.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• May include dependent business interruption as well.</td>
</tr>
<tr>
<td></td>
<td><strong>Data Asset Protection</strong></td>
<td>• Restoration of corrupted data.</td>
</tr>
<tr>
<td></td>
<td>Costs to restore, recreate, or recollect your data and other intangible assets that are corrupted or destroyed by a cyber attack.</td>
<td>• Vendor costs to recreate lost data.</td>
</tr>
<tr>
<td></td>
<td><strong>Event Management / Breach Response</strong></td>
<td>• Forensics.</td>
</tr>
<tr>
<td></td>
<td>Costs resulting from a network security or privacy breach.</td>
<td>• Notification.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Credit Monitoring.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Call Center.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Public Relations.</td>
</tr>
<tr>
<td></td>
<td><strong>Cyber Extortion</strong></td>
<td>• Forensics and related investigation costs.</td>
</tr>
<tr>
<td></td>
<td>Threat to compromise network or data if ransom not paid.</td>
<td>• Costs to negotiate and pay any ransoms demanded.</td>
</tr>
</tbody>
</table>
# Cyber Insurance Overview – Liability Coverages

<table>
<thead>
<tr>
<th>Coverage</th>
<th>Description</th>
<th>Covered Costs</th>
</tr>
</thead>
<tbody>
<tr>
<td>3rd Party insurance coverage:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>privacy liability defense and</td>
<td></td>
<td></td>
</tr>
<tr>
<td>liability incurred for damage</td>
<td></td>
<td></td>
</tr>
<tr>
<td>to others caused by the Insured.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Privacy Liability</td>
<td>Failure to prevent unauthorized access, disclosure or collection, or failure</td>
<td>• Liability and defense costs.</td>
</tr>
<tr>
<td></td>
<td>of others to whom you have entrusted such information, for not properly</td>
<td>• Commercial litigation</td>
</tr>
<tr>
<td></td>
<td>notifying of a privacy breach.</td>
<td>• Consumer litigation – e.g., class-actions.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Third-party costs for notification and investigation.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• PCI fines and penalties.</td>
</tr>
<tr>
<td>Network Security Liability</td>
<td>Failure of system security to prevent or mitigate a computer attack. Failure</td>
<td>• Liability and defense costs.</td>
</tr>
<tr>
<td></td>
<td>of system security includes failure of written policies and procedures</td>
<td>• See above.</td>
</tr>
<tr>
<td></td>
<td>addressing technology use.</td>
<td></td>
</tr>
<tr>
<td>Privacy Regulatory Defense</td>
<td>Privacy breach and related fines or penalties assessed by Regulators.</td>
<td>• Liability and defense costs.</td>
</tr>
<tr>
<td>Costs</td>
<td></td>
<td>• Regulatory investigations.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Civil fines and penalties.</td>
</tr>
</tbody>
</table>
Cyber Insurance Payouts by Coverage

Source: Verizon Data breach report 2016
1. Resulting Bodily Injury / Property Damage
   • CGL or Property insurance *may* provide coverage
   • AIG, AEGIS and some Lloyds syndicates offer coverage for bodily injury / property damage resulting from a cyber attack.

2. Money, Securities or Tangible Property
   • Crime/Fidelity insurance covers computer fraud losses
   • “Social engineering” losses can be expressly covered via endorsement

3. Trade Secrets / Intellectual Property
   • The loss of trade secrets or other intellectual property is not insurable
Cyber Market Overview

**Capacity**
- $970MM in theoretical capacity
- Over 20 markets offer primary coverage, including: AIG, Berkshire, CV Starr, London, Chubb, Zurich, CNA, HCC, Liberty, Beazley, XL, Endurance Swiss Re, AXIS, Nationwide and Travelers.

**Coverage**
- Select insurers provide full limit coverage for first party coverages
- System Failure & Dependent Business Interruption coverages
- 3rd party property damage / bodily injury coverage available offered by AEGIS, AIG and some Lloyds syndicates.

**Appetite**
- In recent years, a more thorough underwriting process has been required for Cyber risks. Underwriters are placing increased scrutiny on Healthcare, Retail and Financial Institutions risks in particular.
- Construction is a favored industry sector for most markets

**Pricing**
- Premium is heavily dependent on security controls, limitations of liability within contracts, retention level, coverage requests, and loss history
- Cyber Liability underwriters have been increasing rate by 0 – 10%, with no change in exposure profile
Key Purchasing Decisions

1. Flexibility Regarding Breach Response Vendors

2. Which Coverages to Purchase?

3. How Much Coverage to Purchase?
   - Benchmarking
   - Marsh’s IDEAL model
   - Contractual requirements

4. Retention?
   - Company risk management philosophy
   - Benchmarking

5. Retroactive Coverage
Marsh Proprietary Benchmarking

**Industry:** Construction  
**Revenues:** All Revenue Bands  
**Peers:** 52 peers
# IDEAL Cyber Model (Sample)

## First Party Costs

<table>
<thead>
<tr>
<th>Event Type</th>
<th>Percentile</th>
<th>PR / Legal</th>
<th>Forensics Investigation</th>
<th>Notification Costs</th>
<th>Call Center</th>
<th>Credit Monitoring</th>
<th>ID Theft Repair</th>
<th>TOTAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mean</td>
<td></td>
<td>$94,225</td>
<td>$276,456</td>
<td>$1,049,471</td>
<td>$269,420</td>
<td>$1,017,389</td>
<td>$1,833,995</td>
<td>$4,540,955</td>
</tr>
<tr>
<td>1 in 2 Events</td>
<td>50%</td>
<td>$74,398</td>
<td>$119,780</td>
<td>$13,211</td>
<td>$3,223</td>
<td>$12,848</td>
<td>$20,212</td>
<td>$262,085</td>
</tr>
<tr>
<td>1 in 4 Events</td>
<td>75%</td>
<td>$90,590</td>
<td>$170,749</td>
<td>$258,023</td>
<td>$62,693</td>
<td>$251,507</td>
<td>$386,790</td>
<td>$1,189,926</td>
</tr>
<tr>
<td>1 in 5 Events</td>
<td>80%</td>
<td>$97,691</td>
<td>$190,748</td>
<td>$544,357</td>
<td>$129,146</td>
<td>$527,949</td>
<td>$799,626</td>
<td>$2,318,044</td>
</tr>
<tr>
<td>1 in 10 Events</td>
<td>90%</td>
<td>$193,882</td>
<td>$971,121</td>
<td>$2,008,155</td>
<td>$495,485</td>
<td>$1,944,639</td>
<td>$3,204,893</td>
<td>$9,136,968</td>
</tr>
<tr>
<td>1 in 20 Events</td>
<td>95%</td>
<td>$222,775</td>
<td>$1,337,055</td>
<td>$5,320,816</td>
<td>$1,331,809</td>
<td>$5,174,014</td>
<td>$8,511,566</td>
<td>$22,146,770</td>
</tr>
<tr>
<td>1 in 100 Events</td>
<td>99%</td>
<td>$257,807</td>
<td>$1,816,190</td>
<td>$5,625,384</td>
<td>$21,423,514</td>
<td>$37,336,291</td>
<td>$87,658,754</td>
<td></td>
</tr>
</tbody>
</table>

## Third Party Costs

<table>
<thead>
<tr>
<th>Event Type</th>
<th>Percentile</th>
<th>Regulatory Fines/Penalties</th>
<th>Consumer Redress Fund</th>
<th>Card Reissuance Liability</th>
<th>Legal Defense &amp; Damages</th>
<th>TOTAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mean</td>
<td></td>
<td>$64,743</td>
<td>$60,441</td>
<td>$3,158,791</td>
<td>$1,367,728</td>
<td>$4,651,704</td>
</tr>
<tr>
<td>1 in 2 Events</td>
<td>50%</td>
<td>$0</td>
<td>$0</td>
<td>$40,164</td>
<td>$6,352</td>
<td>$118,646</td>
</tr>
<tr>
<td>1 in 4 Events</td>
<td>75%</td>
<td>$0</td>
<td>$0</td>
<td>$788,724</td>
<td>$173,714</td>
<td>$1,287,420</td>
</tr>
<tr>
<td>1 in 5 Events</td>
<td>80%</td>
<td>$0</td>
<td>$0</td>
<td>$1,665,990</td>
<td>$406,093</td>
<td>$2,453,054</td>
</tr>
<tr>
<td>1 in 10 Events</td>
<td>90%</td>
<td>$205,421</td>
<td>$0</td>
<td>$6,039,248</td>
<td>$2,260,349</td>
<td>$8,759,651</td>
</tr>
<tr>
<td>1 in 20 Events</td>
<td>95%</td>
<td>$508,204</td>
<td>$6,070</td>
<td>$16,101,270</td>
<td>$6,140,339</td>
<td>$23,026,510</td>
</tr>
<tr>
<td>1 in 100 Events</td>
<td>99%</td>
<td>$1,074,465</td>
<td>$1,097,370</td>
<td>$65,354,350</td>
<td>$31,487,467</td>
<td>$96,964,255</td>
</tr>
</tbody>
</table>
Underwriting Information & Best Practices

• Information on Records
  – Number of records (PII, PHI, PCI)
  – How and where is it stored?
    - On site?
    - Third party vendors?
    - Public/private cloud?

Best Practice: Data encrypted at-rest, in-transit, and on portable devices; access to sensitive data is restricted on a role or business need basis; PII reduction program is in place where applicable

• Loss Experience
  – Have there been any cyber events in the last year?
  – How many and how much information has been exposed?

Best Practice: If the applicant has experienced a data breach, steps have been taken to mitigate against future events/losses
Underwriting Information & Best Practices

• Regulatory Compliance
  – **Best Practice:** Compliant with all regulatory rules/statutes that may govern the industry in which the client operates

• Organizational & Administrative Controls
  – **Best Practice:** Formal policies and a framework is in place for data protection that is communicated to all employees and has been reviewed by a qualified attorney; an established security team structure wherein IT management/data security is separate from IT operations; designated individuals or committees with oversight and responsibility over IT security and privacy

• Electronic Controls
  – **Best Practice:** Updates and patches to security software are completed in a timely manner and proactively monitored; vulnerability scans are performed on all critical systems and deficiencies are properly mitigated and addressed
Underwriting Information & Best Practices

• Physical Security Controls
  – **Best Practice**: Access to static data (file rooms/backup tapes) and servers is restricted to authorized employees at specified entry points

• Security and Privacy Culture
  – **Best Practice**: Network security and data privacy is a board level concern; employees are educated and aware of the importance of data security and understand their personal liability for participating in a data breach incident

• Crisis Management Preparedness
  – **Best Practice**: A pre-planned and well documented incident response plan and escalation plan is in place and enforced

• Business Continuity/Disaster Recovery Planning
  – **Best Practice**: A business continuity and incident response plan is in place, reviewed, tested, and updated continually, and communicated to employees; redundancies are in place to prevent against a total and permanent loss of data/information
**Marsh Cyber Practice**

**Innovate**
Industry leading solutions like Cyber IDEAL and Cyber View.

**Strength in Market**
Placing over $250M in global premiums with leading insurers including AIG, Beazley, Zurich, and Chubb.

**Market Capacity**
Creating capacity in the marketplace, including solutions like Cyber CAT and Cyber ECHO.

---

**MARSH BY THE NUMBERS**

**CYBER CREDENTIALS**

- **25+** Global experts in network security and privacy, E&O and media liability
- **$250M+** Cyber premiums place globally
- **5** Hub locations mapped by key insurer decision makers: NY, SF, Chicago, London, Bermuda
- **1,400+** Network security/privacy and E&O clients
- **90%+** Client retention rate
- **2014, 2015 & 2016** Advisen Cyber Broker of the Year
This document and any recommendations, analysis, or advice provided by Marsh (collectively, the “Marsh Analysis”) are intended solely for the entity identified as the recipient herein (“you”). This document contains proprietary, confidential information of Marsh and may not be shared with any third party, including other insurance producers, without Marsh’s prior written consent. Any statements concerning actuarial, tax, accounting, or legal matters are based solely on our experience as insurance brokers and risk consultants and are not to be relied upon as actuarial, accounting, tax, or legal advice, for which you should consult your own professional advisors. Any modeling, analytics, or projections are subject to inherent uncertainty, and the Marsh Analysis could be materially affected if any underlying assumptions, conditions, information, or factors are inaccurate or incomplete or should change. The information contained herein is based on sources we believe reliable, but we make no representation or warranty as to its accuracy. Except as may be set forth in an agreement between you and Marsh, Marsh shall have no obligation to update the Marsh Analysis and shall have no liability to you or any other party with regard to the Marsh Analysis or to any services provided by a third party to you or Marsh. Marsh makes no representation or warranty concerning the application of policy wordings or the financial condition or solvency of insurers or reinsurers. Marsh makes no assurances regarding the availability, cost, or terms of insurance coverage.