

Premium Summary

COVERAGE	CARRIER	2013-2014 EXPIRING ANNUALIZED PREMIUM	2014-2015 RENEWAL PREMIUM	COMMENTS
Property Engineering Fee	Affiliated FM	\$159,134 \$6,500	\$158,417 \$6,500	Expiring TIV \$435,406,871; rate \$0.0354 Renewal TIV \$433,381,941; rate \$0.0354 Reduction in TIV due to deletion of the Burn Tower
Crime	Great American	\$5,093	\$5,212	New form with more current policy language, coverage matches expiring
General Liability Employee Benefits Liability Sexual Abuse & Molestation	Hanover	\$53,087	\$53,408	
Professional Liability Educator's Legal Employment Practices Law Enforcement	Hanover	\$46,269	\$57,508	Premium up due to recent increase in Employment Practices claim activity
Auto	Hanover	\$40,677	\$40,888	Expiring 31 vehicles, 6 trailers Renewal 31 vehicles, 5 trailers
Umbrella	Hanover	\$44,227	\$44,677	
International Package	ACE	n/a	\$1,250	New coverage
Cyber Liability	AIG	n/a	\$15,781	New coverage
Total Premium		\$354,987	\$383,641	

COMMENTS:

- Premiums include Terrorism

**CYBER LIABILITY
QUOTE OPTIONS**

Description				
Form	Specialty Risk Protector			
Insurer	Illinois National Insurance Company (AIG) (AM Best A XV)			
Coverage Type	Claims Made			
INSURING AGREEMENT	COVERAGE	LIMIT Option 1	LIMIT Option 2	LIMIT Option 3
Security and Privacy Liability Insurance	<ul style="list-style-type: none"> Covers third-party claims arising from a failure of the network security or a failure to protect data. 	\$1,000,000	\$3,000,000	\$5,000,000
Regulatory Action Sublimit	<ul style="list-style-type: none"> Responds to regulatory actions in connection with a security failure, privacy breach, or the failure to disclose a security failure or privacy breach 	\$500,000	\$2,000,000	\$2,000,000
Media Content Insurance	<ul style="list-style-type: none"> Addresses liability related to distributing media content via a website. Coverage for perils including copyright infringement, trademark infringement, defamation and invasion of privacy 	\$1,000,000	\$3,000,000	\$5,000,000
Network Interruption Insurance	<ul style="list-style-type: none"> Responds to a material interruption of business operations caused by a network security failure by reimbursing for lost income and operating expenses 	\$1,000,000	\$3,000,000	\$5,000,000
Event Management	<ul style="list-style-type: none"> Responds to a security failure or privacy breach by paying cost of notifications, public relations, and other services to assist in managing and mitigating a cyber-incident. Forensic investigations, legal consultations, and identity monitoring costs for victims of a breach are included. 	\$500,000	\$2,000,000	\$2,000,000
Cyber Extortion Insurance	<ul style="list-style-type: none"> Responds to the threat of intentional security attacks by an outsider attempting to extort money, securities, or other valuables. Includes monies paid to end the threat and the cost of an investigation to determine the cause of the threat. 	\$1,000,000	\$3,000,000	\$3,000,000
Policy Aggregate		\$1,000,000	\$3,000,000	\$5,000,000
Retention		\$25,000	\$50,000	\$50,000
ANNUAL PREMIUM		\$15,781	\$34,811	\$50,770

COMMENTS:

- Quote subject to receipt of Application Warranty Letter
- Exclusion for failure to encrypt confidential information

CYBER LIABILITY CONT.
MISCONCEPTIONS

Here are some of the more common misconceptions held by public entities concerning their vulnerability:

1. **“Public entities are not a target for cyber-attacks.”** Actually, public entities are a perfect target for cyber-attacks considering the amount of confidential information in their possession. There is probably no other type of organization, other than a bank or financial institution, that stores more personally identifiable information. It's not uncommon for a public entity to have an individual's Social Security number, income statements, bank account numbers, driver's license number and even credit card information. In addition, public entities typically have confidential personal medical and health information for all of their employees.
2. **“We have the latest technology and software available to protect our electronic information and systems.”** The growing number of cyber-attacks (more than 500 million records breached since 2005) at both large and small organizations--even those with the most sophisticated software protection--demonstrates that no organization can be sure they are not susceptible. One of the most common causes of privacy information breaches today is not hacking, but human error. When confidential information is stored outside the network system on laptops, smartphones or other electric storage devices, it can be compromised when the device is lost or stolen.
3. **“Even if our network is breached, we are covered under our general liability or other insurance policies.”** General liability insurance commonly provides coverage for “bodily injury” and “property damage.” Property damage typically means physical injury to tangible property, including the resulting loss of use of that property. However, electronic data is not tangible property and is not covered. In addition, property insurance, crime insurance and professional errors and omissions insurance do not typically provide coverage for cyber liability and notification requirement expenses.
4. **“Cyber liability notification requirements only apply to commercial businesses.”** Currently, in addition to federal regulations, more than 45 states have enacted legislation to protect consumer privacy. These state and federal requirements apply to for-profit and not-for-profit organizations, including public entities. Both state and federal agencies may investigate and take action against any organization that is negligent in the handling of confidential personal information.
5. **“If we had a data breach, we could handle the notification requirements ourselves.”** Most public entities would have difficulty complying with state and federal notification requirements in the event of a data breach. It is also common for goodwill purposes to provide credit monitoring services and identity theft education and assistance for the affected party. Most public entities would not have the expertise and staff to provide these types of additional goodwill services for the affected party.

--From Property Casualty 360° article by John A. Solari April 18, 2012

CYBER LIABILITY CONT.

CLAIM EXAMPLES

Example 1

A laptop containing a data base with Social Security numbers of nearly 7,500 current and former university students was stolen with the password for the data on the hard drive. Several students reported that third parties attempted to activate credit cards in their names. The insurer added its expertise to the insured university with immediate assistance, including call center services, an anti-fraud protection vendor, credit-monitoring services, and counsel. The insurer's quick response enabled the university to provide students with timely services to mitigate the risk of identity theft.

Example 2

A university audit uncovered a security breach which allowed unauthorized individuals to access the financial aid roster including personal data. The insurer's cyber security specialists assisted the university in conducting a forensic audit which determined that more than 18,000 student records may have been compromised. The insurer also helped the university select vendors to provide call center services and credit monitoring. The insurer reimbursed the insured approximately \$70,000 above the retention for the vendors' services.

Example 3

Three credit-card pay station machines were compromised at a large university, and the university's IT department discovered a breach shortly thereafter in the university's network stemming from the pay station incident. The insurer's cyber security specialists stepped in quickly to assist in the investigation. The insurer worked with the insured in retaining a forensic auditor as well as a breach coach and is evaluating the need for credit-monitoring services.

Example 4

A college inadvertently sent an email to approximately 80 students that attached a file containing personal data for all of its students. Working together, the insurer and the college were able to retrieve 55 of the emails before they were opened. The insurer worked closely with the school's dean of students and arranged notification and credit monitoring for the impacted students.

The average cost per record of a data breach in the United States is \$188, including direct (forensics, hotline support and credit monitoring) and indirect costs (loss of clients, employee time.)

--Ponemon 2013 Cost of a Data Breach Report

INTERNATIONAL TRAVEL QUOTE OPTION

Description	
Form	International Advantage
Insurer	ACE American Insurance Company (AM Best A++ XV)
COVERAGE	LIMITS
Contingent Automobile Liability Coverage Form	
Each Accident (Covering Owned and Hired & Non-Owned Autos)	\$1,000,000
Hired Auto Physical Damage – Each Accident / Each Policy Period	\$50,000 / \$50,000
Employers Responsibility Coverages	
Benefits for Voluntary Compensation: North Americans: Third Country Nationals: Local Nationals:	State of Hire Not Covered Not Covered
Executive Assistance Services (Including Repatriation): Medical Assistance Services Policy Limit	\$1,000,000
Employers Liability: Bodily Injury by Accident – Each Accident Bodily Injury by Disease – Including by “Endemic Disease” – Each Employee Bodily Injury by Disease – Including by “Endemic Disease” – Policy Limit	\$1,000,000 \$1,000,000 \$1,000,000
Accidental Death & Dismemberment and Medical Coverage	
Coverage A: Accidental Death & Dismemberment – per covered persons	\$50,000
Coverage B: Medical Expense – per covered persons	\$10,000
Aggregate Limit of Liability	\$1,500,000
ANNUAL PREMIUM	
	\$1,250

EXECUTIVE ASSISTANCE SERVICES INCLUDE:

- E-Services including pre-trip security, health and travel information
- Live services including 24 hour access while traveling worldwide
- Emergency medical, personal, legal and travel services
- Emergency medical evacuation or repatriation services
- Concierge service

EDUCATOR'S LEGAL & EMPLOYMENT PRACTICES LIABILITY
CLAIM DETAIL

DATE OF LOSS	CLAIM No.	CLAIM DESCRIPTION	STATUS
8/19/2014	15-00391543	Claimant alleges she was subjected to discipline, harassment, and discharge because of disabilities	Closed
7/18/2014	15-00369700	Multiple claimants alleging retaliation	Open
7/15/2014	15-00369590	Claimant alleges that she was subjected to discrimination based on disability and retaliation	Open
4/16/2014	15-00369294	Claimant is alleging discrimination based on retaliation and disability	Open
3/28/2013	15-00064265	EEOC complaint alleging discrimination	Closed

BENCHMARKING

ENTITY	LIMIT	RETENTION/DEDUCTIBLE	ESTIMATED PREMIUM (INCLUDING UMBRELLA)
Collin	\$5,000,000	\$25,000	\$66,771
DCCCD	\$5,000,000	\$100,000	\$168,960
Tarrant County Community College	\$7,000,000	\$75,000	\$87,594
Alamo Colleges	\$4,000,000	Not known	\$156,078

PROPERTY BENCHMARKING

ENTITY	TOTAL INSURED VALUE	LOSS LIMIT	AOP DEDUCTIBLE	WIND/HAIL DEDUCTIBLE	RATE	CARRIER
Collin	\$433,381,941	n/a	\$50,000	\$50,000 per location	\$ 0.037	Affiliated FM
A	\$893,726,472	\$500,000,000	\$100,000	\$100,000 per location, \$500,000 agg occ	\$ 0.049	Lexington
B	\$950,000,000	\$100,000,000	\$100,000	\$250,000 per occurrence	\$ 0.48	TASB
C	\$967,842,095	\$500,000,000	\$100,000	\$500,000 per occurrence	\$ 0.06	Travelers
D	\$1,300,000,000	\$500,000,000	\$100,000	Not known	\$ 0.065	Affiliated FM
E	\$616,791,731	n/a	\$100,000	\$100,000 per locations, \$500,000 agg occ	\$ 0.042	TASB
F	\$800,000,000	n/a	\$100,000	\$100,000 per occurrence	\$ 0.049	TASB
G	\$333,203,095	\$250,000,000	\$25,000	\$25,000 per occurrence	\$ 0.054	Fireman's Fund
H	\$253,864,506	n/a	\$50,000	\$50,000 per occurrence	\$ 0.09	TPS

- Please note program structures including rate and deductibles may differ based on a number of factors including but not limited to claim history, specific county location and type & age of construction.