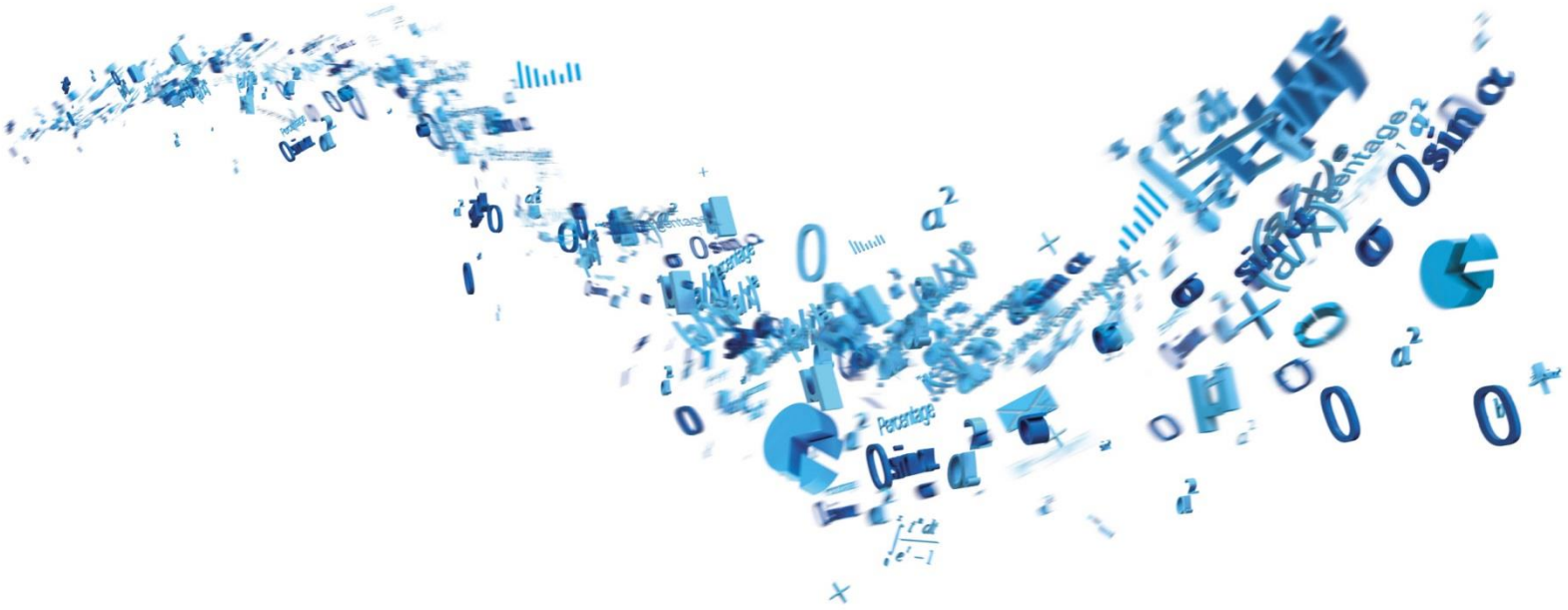
Aon Risk Solutions
Specialty
Professional Services



Cyber and Fidelity Insurance Report for Real Estate Brokers

Empower Results®

Notice

This document is furnished to you as a matter of information for your convenience. It only summarizes information and is not intended to reflect all available information available. Moreover, the information contained in this document reflects proposed coverage and information obtained in the market place . This document is not an insurance policy and does not amend, alter or extend the coverage afforded by Insurers, any other carriers or proposed policy(ies) of Insurers. The information herein is purely information and should not be used as on an individual basis. Each risk is underwritten individually and each risk may vary significantly from one another. This document is purely for information purposes only and should be accepted as such.

Real estate transactions are a target for sophisticated fraud scams and when the frauds succeed, often all the service providers are potential litigation targets. The National Association of REALTORS® would like to identify providers that offer insurance for these threats and then compare the insurance offerings. Three different types of insurance coverages may be needed to protect the brokerage from these threats: Errors & Ommissions/Miscellaneous Professional Liability Insurance ("E&O" or "MPLI"); Cyber Insurance; and Crime Coverage (see Notes at end defining each insurance product).

Exposure Analysis

Real estate brokerages are comprised of independent contractor salespeople. The salespeople may be responsible for their own insurance needs. Because of the many ways brokerages are structured, providing one universal insurance solution for brokerages is not possible.

Since there is no universal solution, we will examine how various lines of coverage respond to the fraud scheme. In the typical scheme, a party to the transaction receives fraudulent information from a fraudster impersonating another participant in the transaction such as the seller. The party may then provide the incorrect instruction to a third party, bank or lawyer, who uses the information to direct the payment to the fraudster's banks account, which leads to a loss. This type of scheme is known as "Social Engineering Fraud."

The real estate professionals will not incur the loss themselves from the fraud scheme. However, they may be involved in the suit for the loss sustained. If it is found that the salesperson was negligent because the fraudster breached the brokerage's computer network to gather intelligence about the transaction, the E&O policy should provide a defense to the salesperson and the brokerage. However, the lost funds will not be covered by the brokerage's E&O insurance as discussed in the next section because the salesperson was not the party making the fund transfer

Coverage Discussion

Businesses are facing an endless stream of attempted and often successful deceptive funds transfers. Although insured's instinctively think of these as "cyber losses," they have not been covered by most cyber insurance policies or crime policies. There are at least seven potential scenarios for deceptive funds transfers:

1) The transfer is effected entirely by a hacker independently penetrating a computer system or a user's personal device like a smart phone, and making the transfer;

2) The hack and transfer are enabled by employee negligence;

3) The fraudster convinces an employee to reveal credentials, enters the network by using them, and then transfers funds;

4) The fraudster gets an employee to open an attachment or click on a link, thereby allowing the network to be penetrated, and allowing the transfer of funds;

5) The fraudster, through emails or telephone calls or both, posing as a company's executives, vendors or customers, convinces an employee to transfer funds;

6) An employee enters data believed to be accurate, but which in fact is fraudulent; and

7) A rogue employee makes an improper transfer or enters fraudulent data.

Numbers 3, 4 and 5 are variants of methods which have come to be known as "social engineering," a term for the manipulation of humans into performing acts or divulging confidential information. However, the "social engineering," coverage that insurance companies are providing only covers a loss where the financial loss has been sustained by the entity making the payment based on the fraudulent information. Since real estate brokerages are usually not the party transferring the funds, the social engineering insurance currently available in the market will not protect them in these instances if they are sued for a third-party loss. Cyber and Crime insurers provide coverage for first-party expenses (or, the insured's expenses) from theft or loss of data but do not protect against third-party losees

Potential Coverage Solution

We have scoured the market and have not established a dedicated miscellaneous professional liability ("MPL") or E&O product that provides Social Engineering coverage that extends to third party losses. From the research we've done, real estate professionals, like most other professionals, would only be able to obtain this coverage for this fraudulent scam through endorsements for other types of insurance products, like a Crime Policy or Cyber policy. However, coverage for third party losses for Social Engineering fraud is not generally available.

Also, each carrier, almost 50 of them in the market, provides a unique and specified E&O Form for each state. To compare all the policy forms is practically impossible.

In short, we suggest the following:

- Each real estate professional should ensure that they have the following insurance coverage for themselves as a minimum: E&O insurance with either a Cyber endorsement or a separate Cyber policy, and the real estate professional may also may need a Crime policy.

- Real estate professionals should make sure the coverage is tailored to their needs. If the real estate professional is holding funds in a transaction, then Crime coverage for is needed. If the real estate professional is not holding funds, then the MPL policy will provide a defense against negligence allegations. However, no coverage is likely available to a real estate professional for a third-party loss of funds that resulted from the Social Engineering Fraud.

The most common way of getting Social Engineering covered is through adding an endorsement to a Crime policy which is available through most major carriers including: Chubb, Travelers, Hiscox, CNA, Hanover, Hartford, Zurich and AIG. Most limits are from $100k up to $250k, but the coverage is available only for first-party losses.

Endurance, CNA, and Lloyd's syndicates have extension endorsements to their Cyber Policies; however, this coverage is limited to first party recovery of transferred funds because of social engineering fraud. Limits available are generally$100k to $250k, but with underwriting can be increased to $500k or $1m.

The actual offer of coverage is determined at the carrier and agent level. This is just a summary of what is potentially available in the marketplace. All insurance programs and coverages should be discussed with your broker of record.

Note(1): MPL (Miscellaneous Professional Liability) or Real Estate Agents Errors & Omissions are the two coverage forms where an individual broker can secure the coverage for their Professional Liability. The policy will contain the coverage terms and restrictions.

Note(2): Crime Coverage is insurance to manage the loss exposures resulting from criminal acts such as robbery, burglary and other forms of theft. It is also called "fidelity insurance". This coverage can be added to the MPL/Real Estate E&O through endorsing the coverage to the policy.

Note(3): Cyber Coverage is an insurance product used to protect businesses and individual users from Internet-based risks, and more generally from risks relating to information technology infrastructure and activities. Risks of this nature are typically excluded from traditional commercial general liability policies or at least are not specifically defined in traditional insurance products. This coverage can be added to the MPL/Real Estate E&O through endorsing the coverage to the policy.

Appendix
Cyber Insurance

Cyber Coverage is usually divided into 2 parts; Liability Coverage and First Party Benefits

Liability Coverage:

Usually, the cyber policy is in conjunction with and E&O policy. If a Real Estate Broker already has and E&O policy these coverage's may be available by endorsement on the E&O policy. The coverage should be able to by default to provide these coverage's as default coverage's:

- Privacy Liability
- Privacy Regulatory Liability
  - Regulatory Fines and Penalties (Sublimit)
- Security Liability
- Media Liability

First Party Benefits:

- Breach Notification Expenses
- Breach Mitigation Expenses
- Crisis Management Expenses
- Business Income and Extra Expenses
- Data Restoration Expenses
- Network Extortion Expenses

Key Coverage that should be highlighted when trying to obtain Cyber Coverage is:

- Privacy coverage for unauthorized access or use of private data in any form including accidental dissemination and vicarious liability for third party vendors.
- 1st Party coverage for Breach Notification and Mitigation expenses assumed under business associate agreement or similar contract.
- Coverage for voluntary Breach Notification expenses with Insurer's consent.
- Coverage for Privacy Regulation fines & penalties and punitive damages, all subject to an insured friendly choice of law provision.
- Privacy coverage extends to vicarious liability for breaches of third party information custodians acting on behalf of the Insured.
- Flexible Breach Mitigation Expense coverage that can be tailored to the type of data compromised.
- Media Offense coverage that extends to content posted on behalf of the Insured on third party sites.
- Coverage for the breach of Non-Public Personal Information or proprietary business information in any form.

Aon Risk Solutions
Specialty
Professional Services

Cyber Policy Marketplace

Capacity	Coverage	Claims & Losses	Retentions	Pricing
Capacity is continuing to grow across geographies	**Coverage continues to evolve and become more valuable for Insureds**	**Stronger data is being gathered as more breaches are reported**	**Retentions are *generally* trending upwards**	**Pricing trends are beginning to stabilize**
Over 65 unique Insurers providing E&O / Cyber capacity Capacity is available domestically (primary and excess), in the U.K. (primary and excess) and in Bermuda (excess only, generally attaching above $50M) From a primary perspective, there continues to be a growing number of Insurers developing appetites for large, complex risks There is over $500M in theoretical capacity available in the E&O/Cyber marketplace	Coverage breadth and limit availability continues to expand Insurers continue to differentiate their offerings with new or enhanced coverage components Breach response coverage continues to increase and expand to meet Insured's needs Insurers continue to build out pre-breach offerings as part of their policy package	Complexity of breaches has driven an increase in incident response expenses incurred by Insureds Claims and loss data has expanded coverage offerings and improved actuarial data for loss modeling purposes Increasingly punitive legal and regulatory environment Plaintiff's bar continues to advance proof of "damages" theories in security/privacy context Open privacy-related litigation can take years to conclude	Retentions of all levels are available in the market, but can vary greatly based on industry class, size and unique exposures Adjusting retentions *can* lead to increased coverage and/or limit flexibility pricing flexibility	Depending on loss history and claims experience, pricing has begun to stabilize due to large readjustments that took place in prior years Renewal premiums are falling in line with the change in exposure levels Excess rate environment continues to firm Some Insureds have secured significant coverage improvements as a result of paying higher premiums

Cyber Purchasing Trends by Industry

Limit trends

- Companies in a number of industries, including financial institutions, hospitality, healthcare, retail, manufacturing, technology, media and transportation, are seeking higher limits options
- For other industries, many organizations are still evaluating the purchase of Cyber insurance or use of their captive to provide Cyber cover due to regulatory, contract, D&O, benchmarking/loss information and financial statement pressures, among other reasons

More new buyers

- Manufacturing, critical infrastructure, pharmaceutical/life sciences, industrials & materials/automotive, public sector, energy/power, higher education, real estate/construction, agribusiness and transportation/logistics industries saw the biggest uptick in new cyber insurance purchases in 2016
- Major concern in these industries is business interruption loss and reliance on technology

Shifting focus on cyber risk exposures

- In prior years, organizations' primary cyber concern was related to privacy breaches
- In 2016, more clients across all industries have focused on business interruption coverage, including systems failure cover, cyber extortion and digital asset restoration
- Cyber insurance cases where courts upheld denial of coverage demonstrate the critical importance of matching customized policy wording to match specific insured cyber exposures

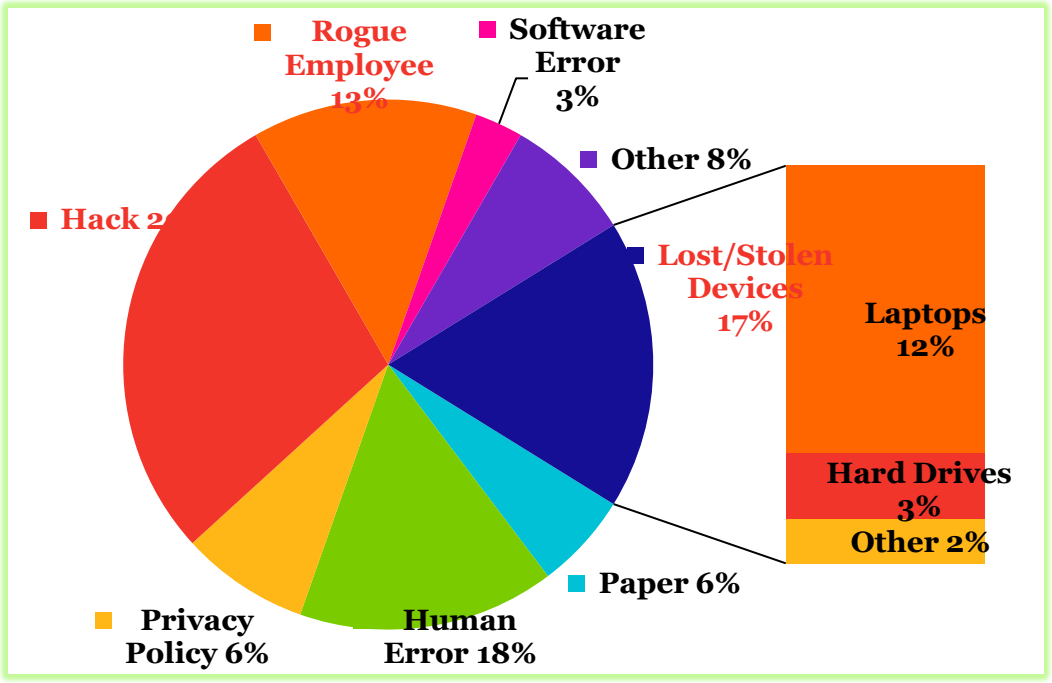
Aon's primary markets used for Cyber.

•AIG	•BCS	•Nationwide	•RLI
•Allianz	•Beazley	•Hartford	•RSUI
•Arch	•Berkshire Hathaway	•HCC	•SCOR Re
•Argo	•Chubb/ACE	•Hiscox	•Swiss Re
•Aspen	•CNA	•Ironshore	•Travelers
•AXIS	•CV Starr	•Liberty Mutual	•XL- Catlin
•AWAC	•Endurance	•QBE	•Zurich

The aforementioned manifest the Insurance Industry appetite for Cyber offerings and the buyer's fortunate position to have many options to choose from at this point. Supply and demand is at healthy levels which is driving price down at this point.

Below we provide, some data as it relates to data hacks, compromises and errors. This data is reflective of how Cyber may have a real influence on your life if left untreated. Especially if Cyber plays a role in generating your income where you have access, even so limited, to other people's/business's data.

Cyber Claims and Industry Trends - 10 years
Claim Trends

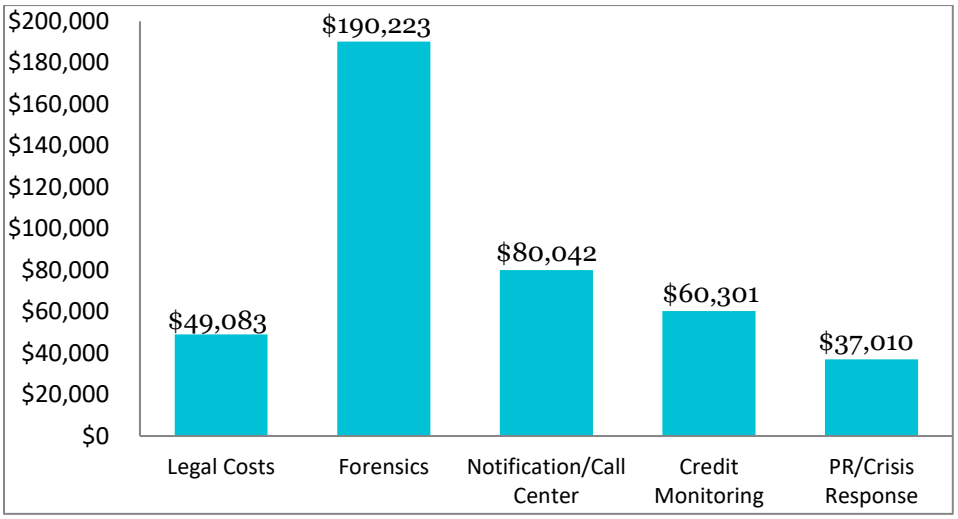


Industry Breakout:

- Healthcare – 32%
- Professional Services – 14%
- Technology- 10%
- Retail – 9%
- Education - 7%
- Travel & Hospitality - 7%
- Financial Institutions - 6%
- Media – 4%
- Non-Profit – 3%
- Public Entity – 2%

Cyber Claims Overview - 10 years

Average Cost of First Party Expenses



Cyber Claims Overview - 3 years

Average Cost of First Party Expenses