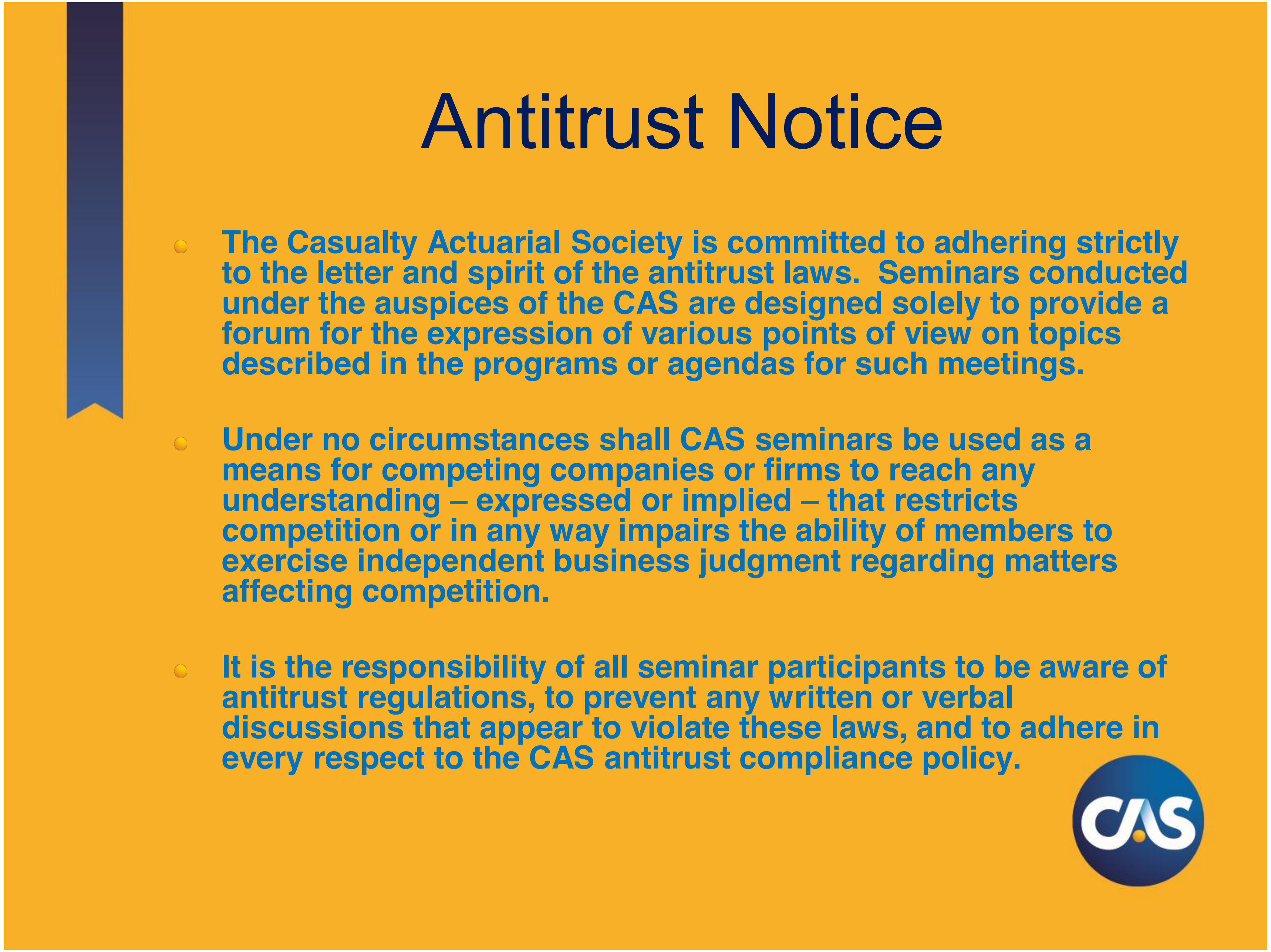
GUIDEWIRE

# Model Data Breach Risk under Catastrophe Model Framework

November 2019



# Antitrust Notice

- The Casualty Actuarial Society is committed to adhering strictly to the letter and spirit of the antitrust laws. Seminars conducted under the auspices of the CAS are designed solely to provide a forum for the expression of various points of view on topics described in the programs or agendas for such meetings.
- Under no circumstances shall CAS seminars be used as a means for competing companies or firms to reach any understanding – expressed or implied – that restricts competition or in any way impairs the ability of members to exercise independent business judgment regarding matters affecting competition.
- It is the responsibility of all seminar participants to be aware of antitrust regulations, to prevent any written or verbal discussions that appear to violate these laws, and to adhere in every respect to the CAS antitrust compliance policy.

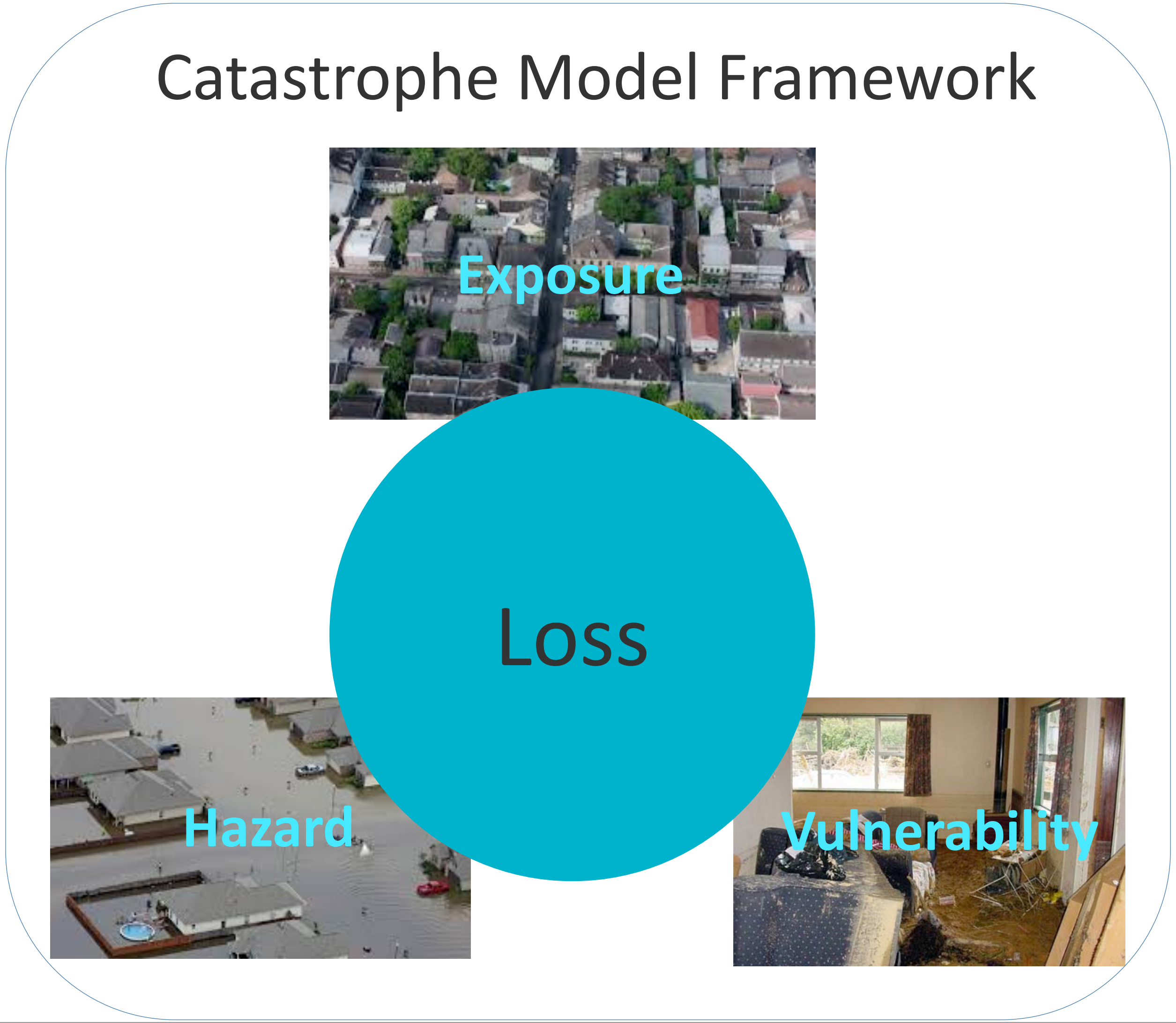
# Data Breach Risk Overview

- Data breach (DB) incident
  - unintentional disclosure of sensitive data from organizations, lead to identity and IP theft, financial fraud, and cyber extortion
- "One massive hack after another"
- Severe consequences for consumers and organizations:
  - direct loss: investigation, notification of victims, credit monitoring, regulatory fines, etc.
  - indirect loss: revenue losses from business disruption, customer turnover, reputational damage

- 2018 Cyber Claims Study (by NetDiligence):
  - total cost ranged from $110 to $80M for 1201 cyber claims in 2013-2017 (companies <$2B in revenue)
- 2019 Cost of a Data Breach Report (by Ponemon Institute):
  - the average total cost of a data breach in the U.S. has grown from $3.5 M in 2006 to $8.2 M in 2019

# Use NAT-CAT Model Framework

- CAT DB event, a man-made CAT event
    - "technological equivalent of extreme weather"
- Heavy tailed distribution of data breach is similar to those of the extreme NAT CAT events.



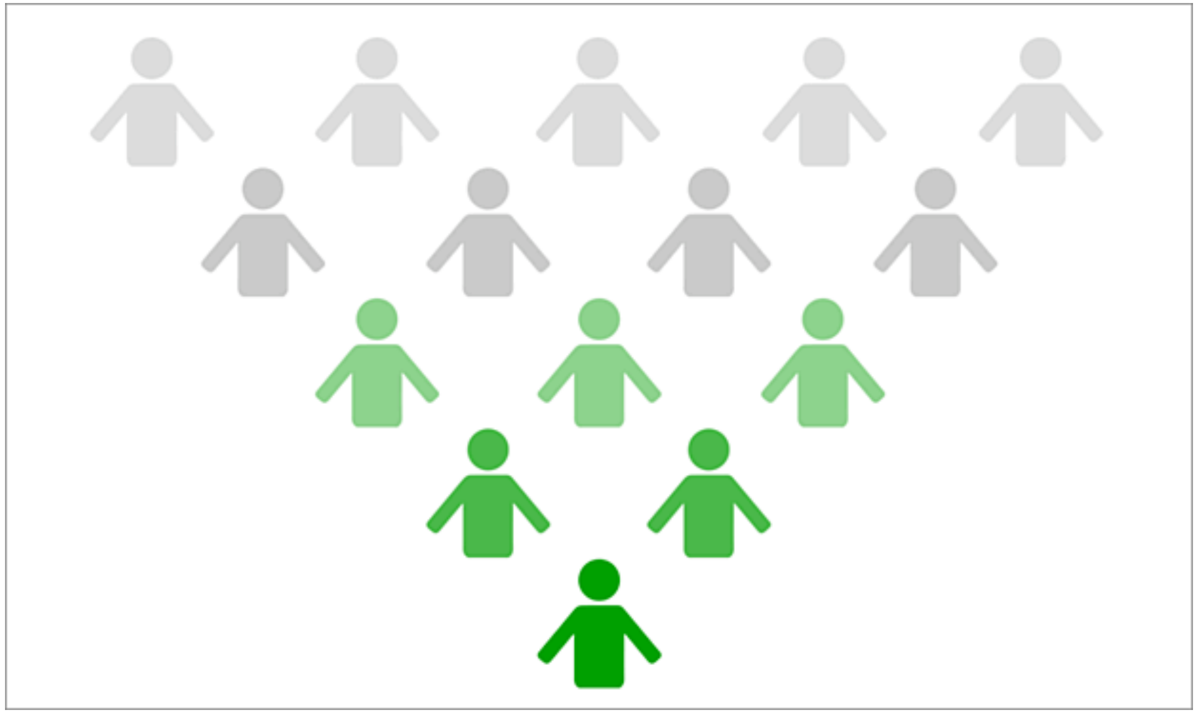
# Data Breach Risk Modeling in CAT Framework

- Exposure: quantity, type, and value of record at risk
- Hazard: threat that may lead to a data breach event
  - Frequency: learned from historical incidents
  - Attackers: internal, external, or more sophisticated actors such as hacktivists
- Vulnerability: damage ratio to total record
- Damage: affected record count
- Loss: cost of an event

Catastrophe Model Framework

Exposure
Loss
Hazard
Vulnerability

# Exposure: total record count = employee + user count



*Utilities*

verizon

COMCAST

*Software & Tech.*

Uber

facebook

*Hospitality*

priceline

MARRIOTT

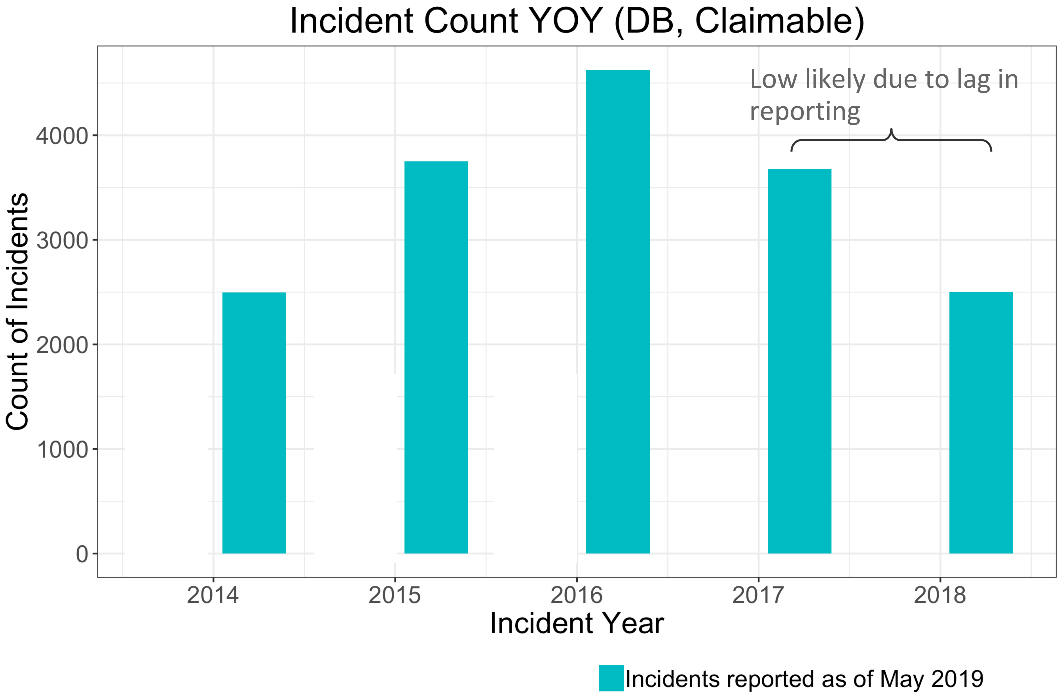
*Financial services*

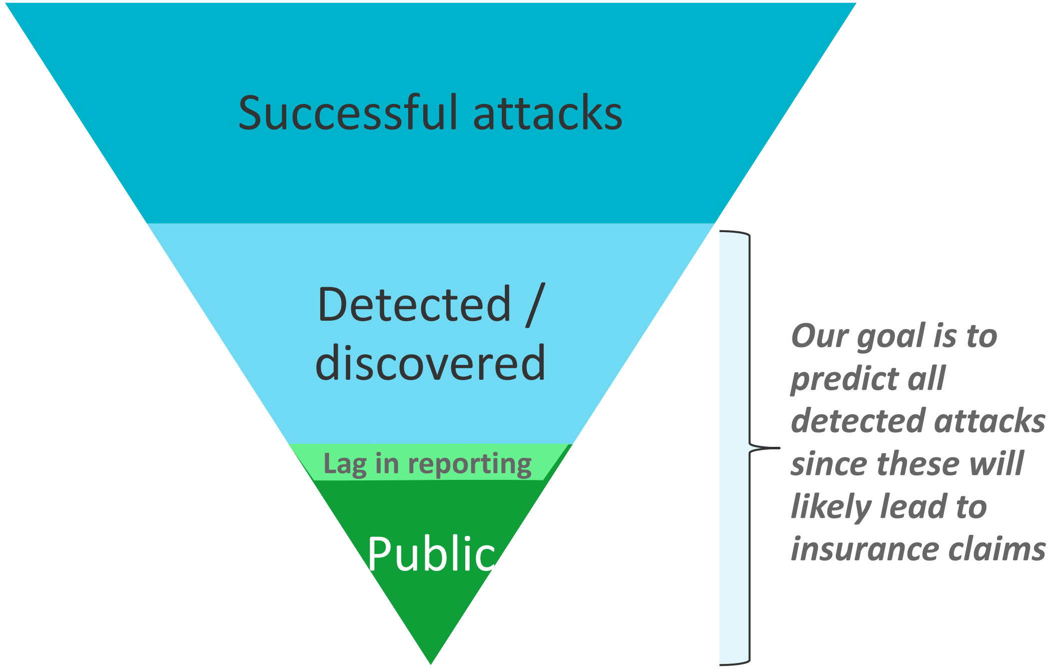
J.P.Morgan

Anthem.

# Hazard: events that lead to data breach

- **Event Frequency:**
  - Evolving landscape
  - Lag in reporting
  - Zero-inflated model is applied

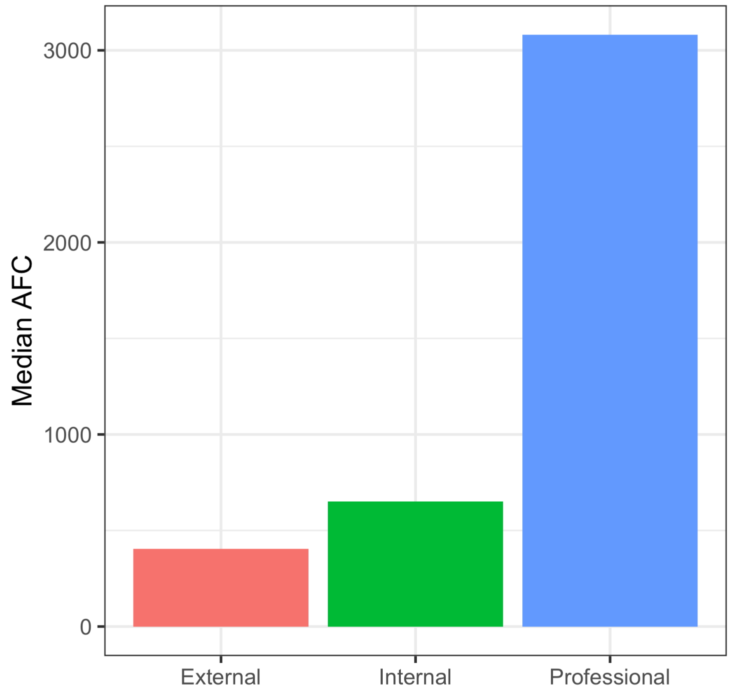




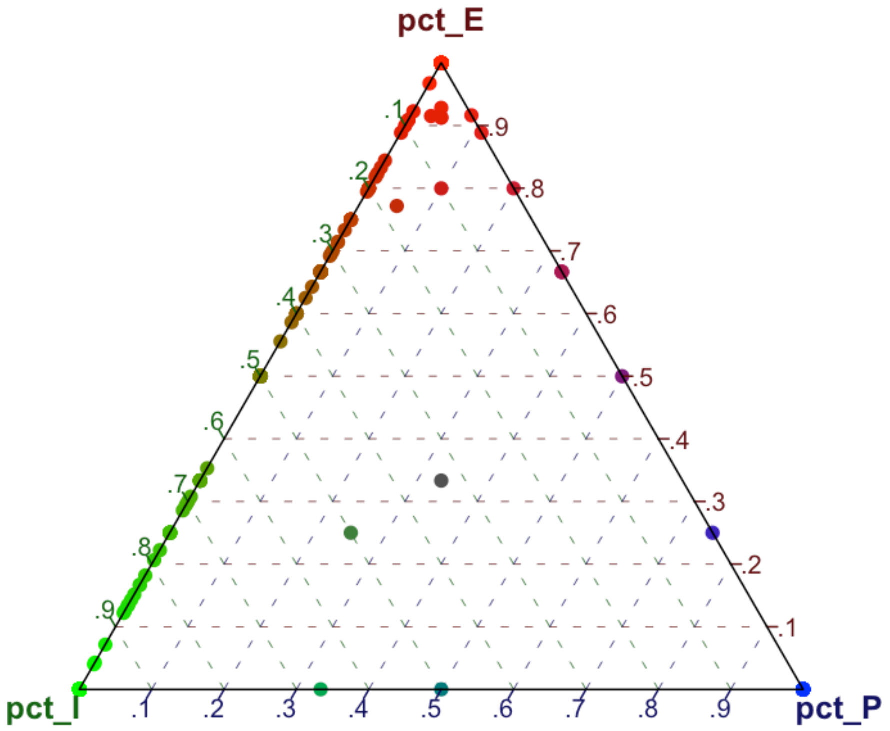
*Our goal is to predict all detected attacks since these will likely lead to insurance claims*

# Hazard: events that lead to data breach

- **Attackers**
  - **Professional**: hacktivist, terrorist, and criminal organization
  - **External**: former employee, former consultant, vendor, etc.
  - **Internal**: employee, consultant, trusted third party, organization, etc.



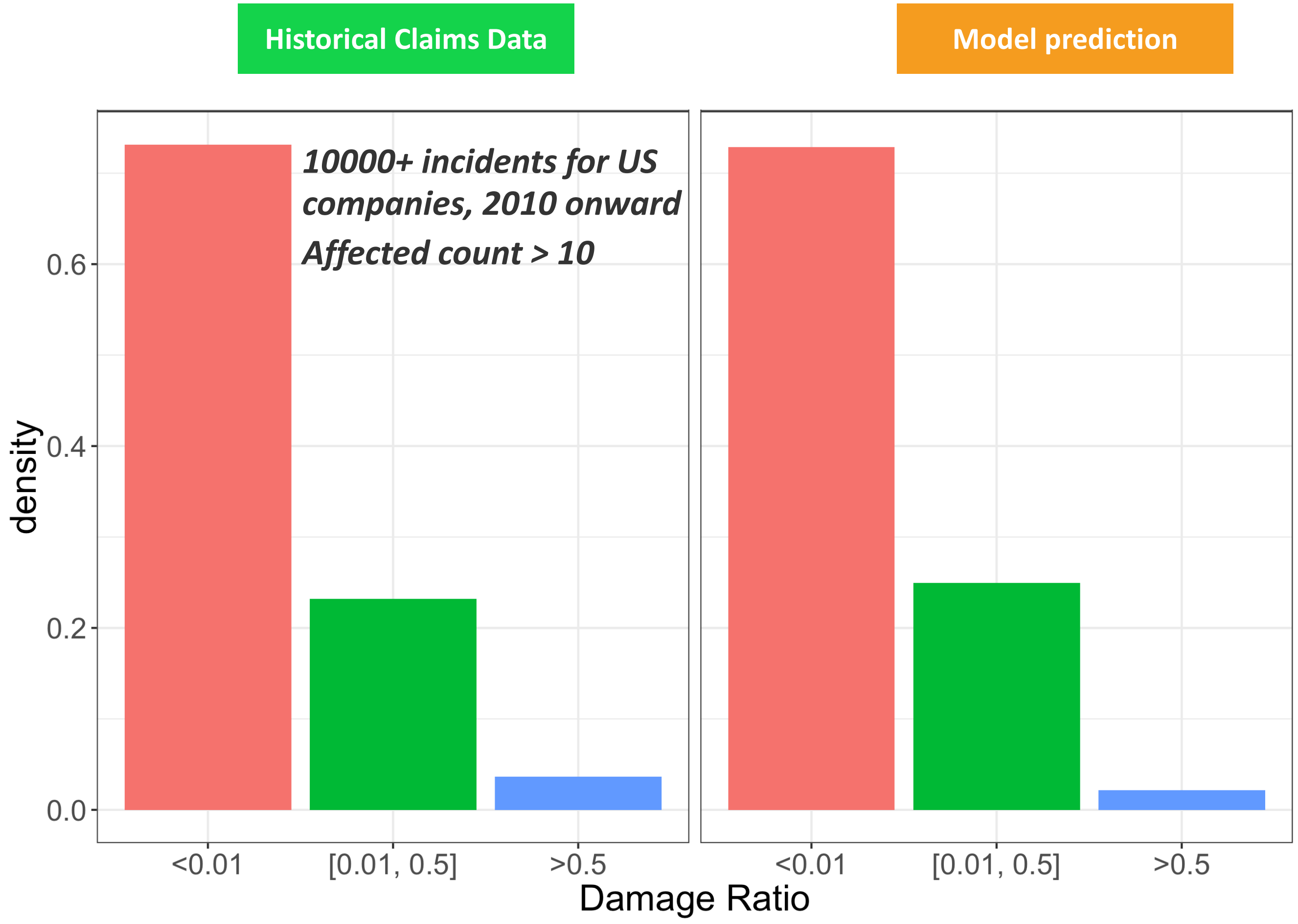
- **A predictive model for the probability of attacker type**
  - Attributes include …



**probability of a company being attacked among the three attacker types (historical incidents for companies)**

# Vulnerability: damage ratio to exposure

- Damage ratio (DR) definition
- Analysis of historical incidents reveals ...
- How to model DR

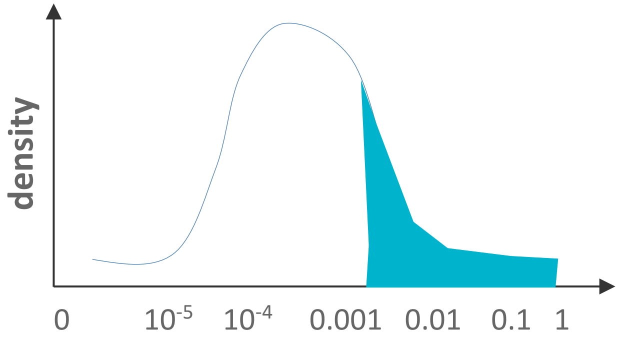


***10000+ incidents for US companies, 2010 onward***

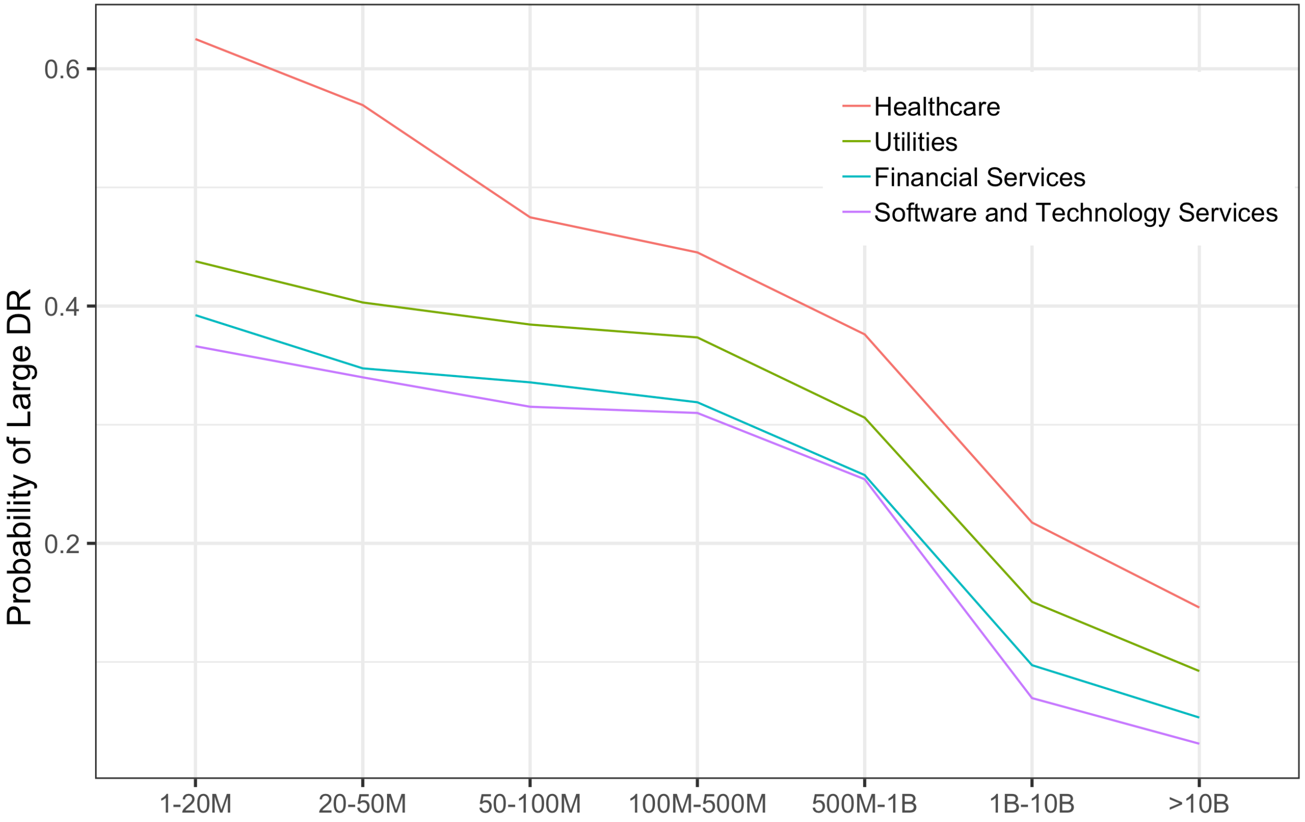
***Affected count > 10***

# Vulnerability: damage ratio to exposure

- Probability of large DR

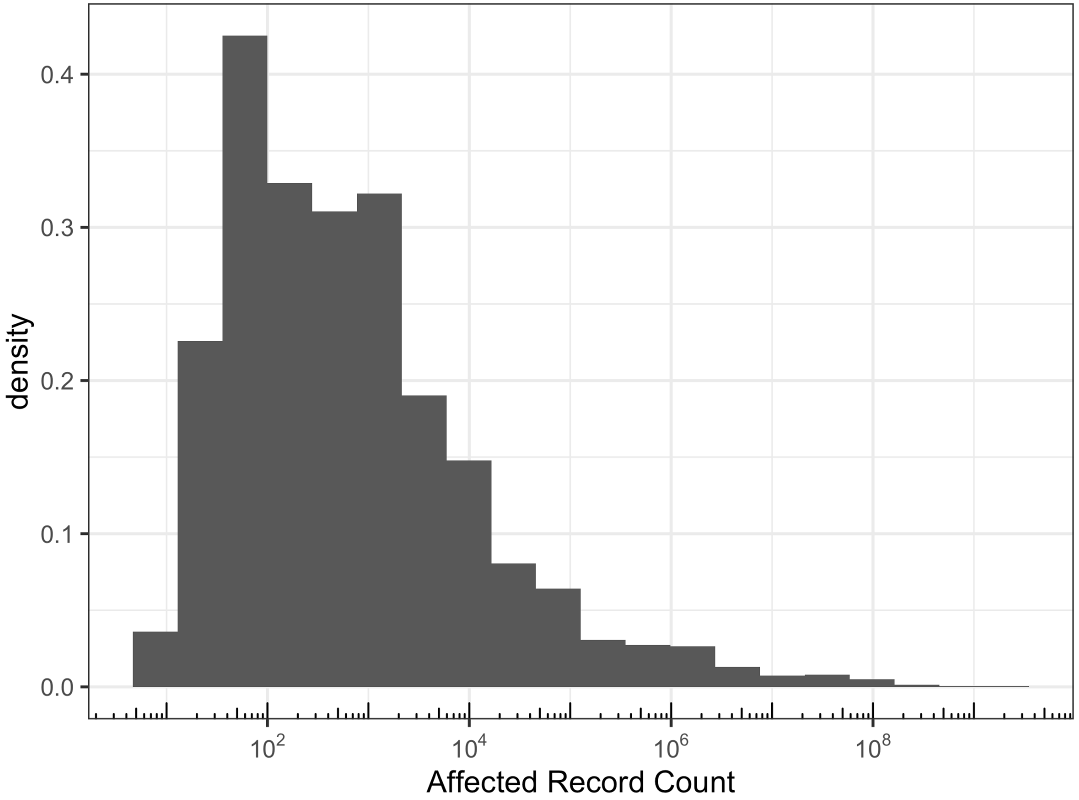


- Variation among industry sectors
- Variation among revenue bins
  - Smaller companies are more likely to have less preventative measures and therefore data is less distributed
  - Larger companies segment network and data and therefore have a lower likelihood of losing a large number of records



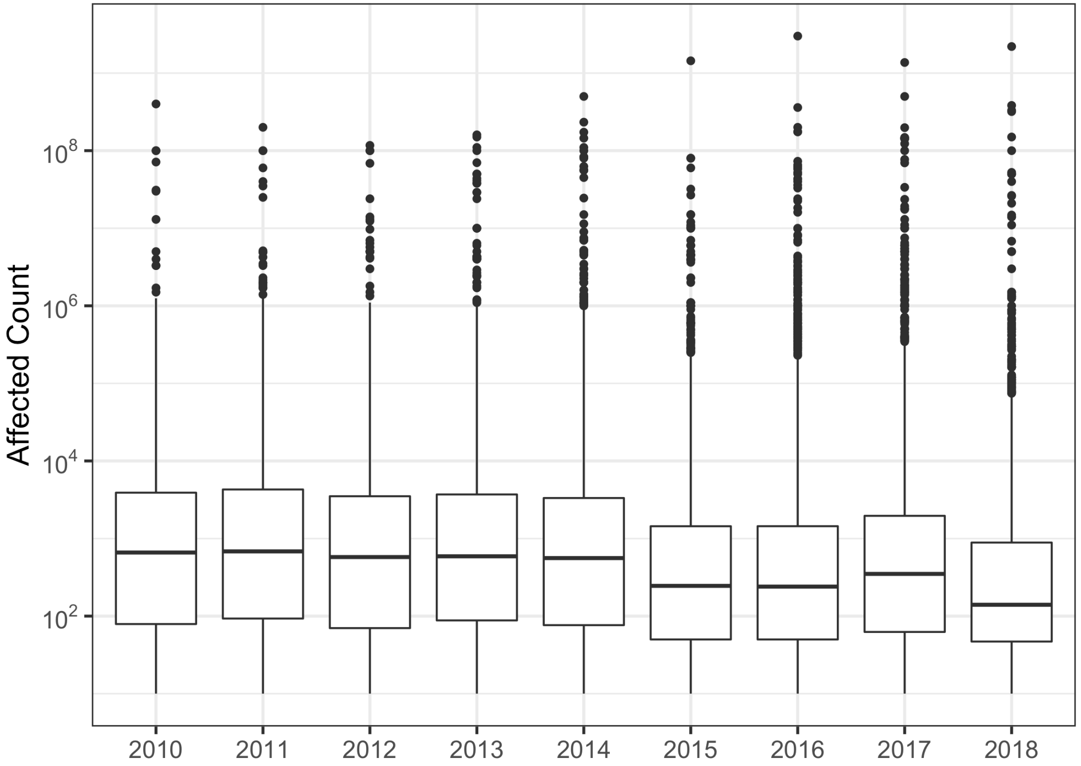
# Damage:
# affected record count = total record count x damage ratio

- Historical data of data breach size



**Histogram of AFC for data breach incidents occurring to US companies in 2009-2018 with AFC > 10**

- Size of data breach is not really increasing over the past decade

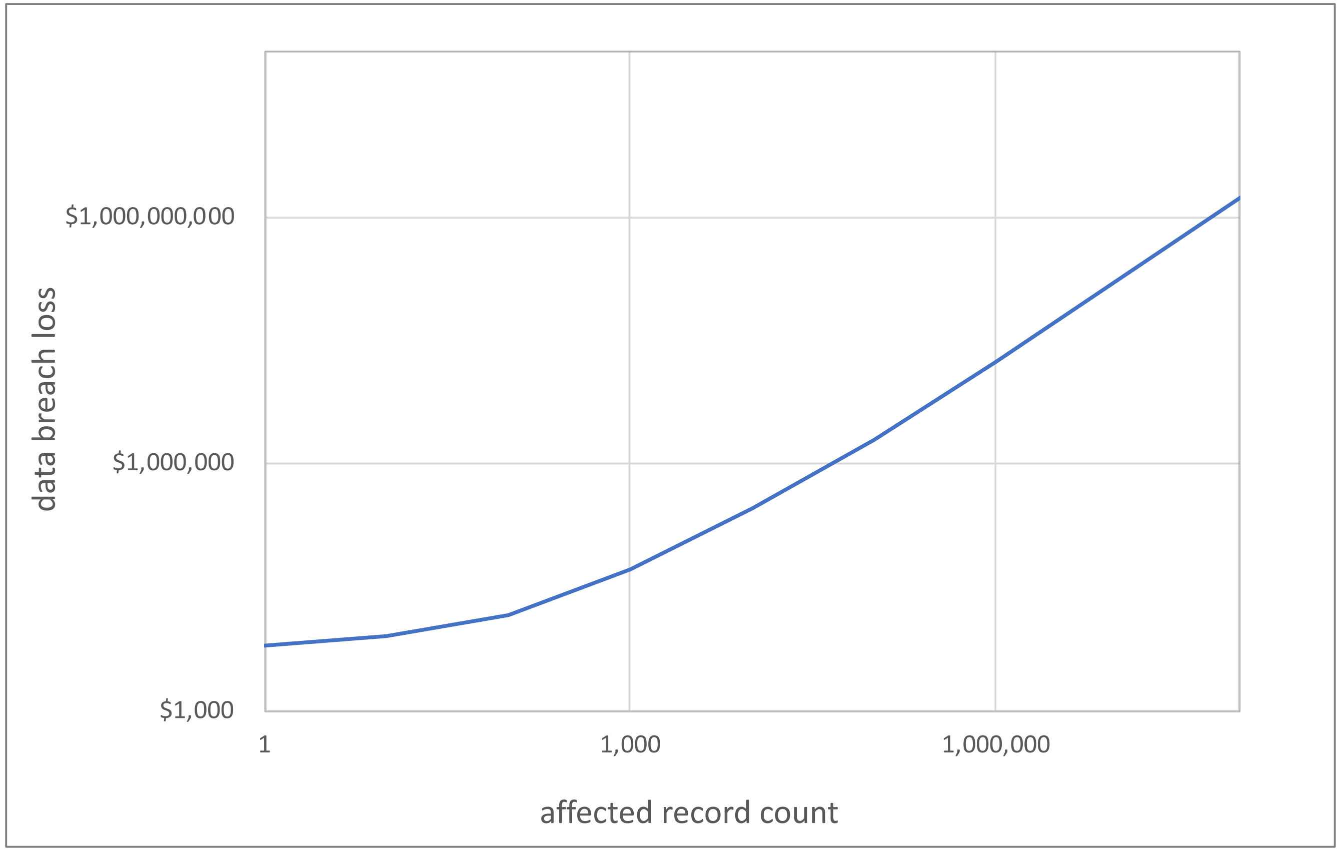


**Yearly change of AFC for data breach incidents occurring to US companies in 2009-2018 with AFC > 10**

GUIDEWIRE

# Loss estimation

- **Loss**
  - investigation costs,
  - notification and post event response costs,
  - regulatory fines and penalties
- **Loss varies with**
  - affected record count
  - type of record (PCI, PHI, PII)
  - country or region
  - data breach history (first time breach ?)

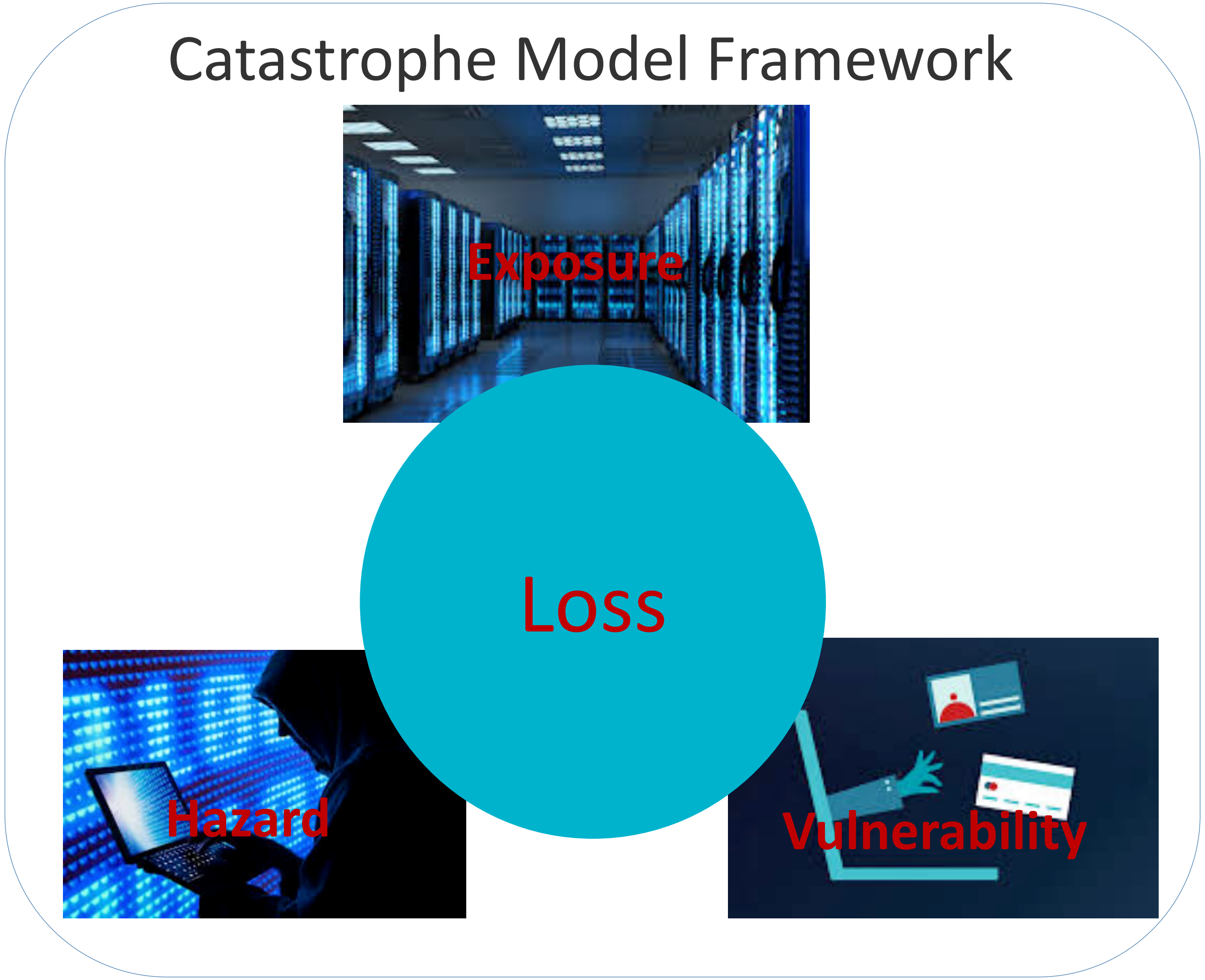


**Example: the relationship between data breach cost and affected record count for PCI data type**

# Data Breach Risk Modeling in CAT Framework

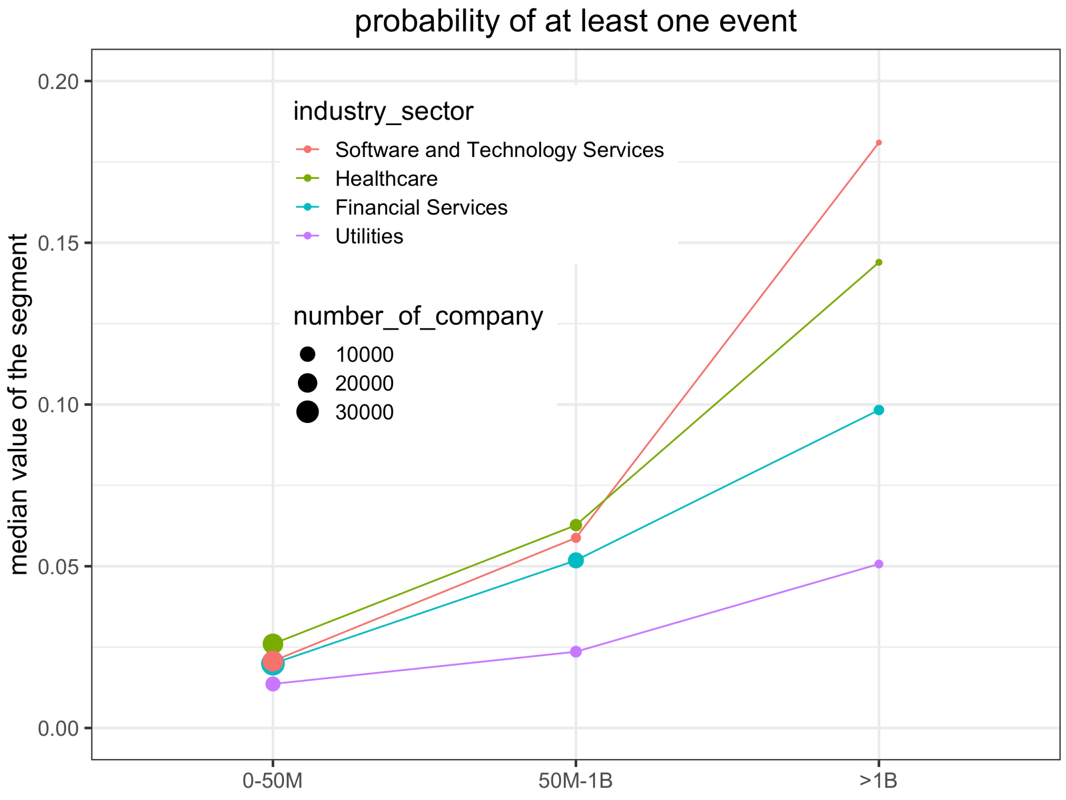
- Exposure: quantity, type, and value of record at risk
- Hazard: threat that may lead to a data breach event
  - Frequency: learned from historical incidents
  - Attackers: internal, external, or more sophisticated actors such as hacktivists
- Vulnerability: damage ratio to total record
- Damage: affected record count
- Loss: cost of an event

Catastrophe Model Framework



# Model Implication

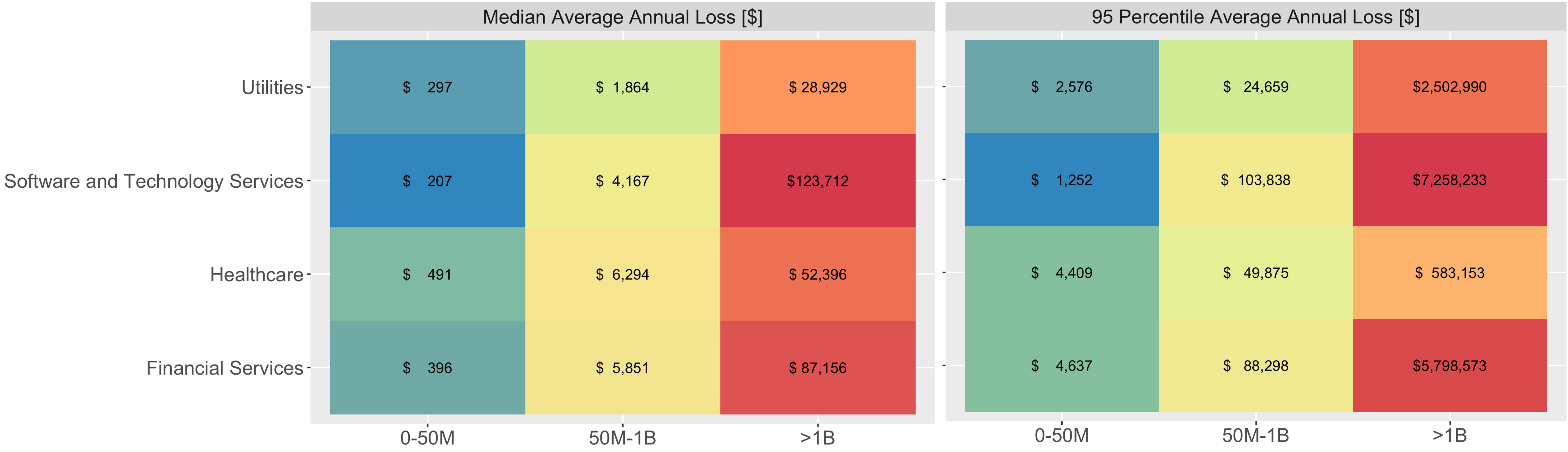
- Predict the likelihood of breaches of a particular size in the coming year, e.g. when a company loses a certain proportion of its total record



Median value of each segment (selected sectors)

# Model Implication

- Provide views of financial loss due to data breach events on both an event-by-event and annual basis



Median Average Annual Loss [$]

| | 0-50M | 50M-1B | >1B |
|---|---|---|---|
| Utilities | $ 297 | $ 1,864 | $ 28,929 |
| Software and Technology Services | $ 207 | $ 4,167 | $123,712 |
| Healthcare | $ 491 | $ 6,294 | $ 52,396 |
| Financial Services | $ 396 | $ 5,851 | $ 87,156 |

95 Percentile Average Annual Loss [$]

| | 0-50M | 50M-1B | >1B |
|---|---|---|---|
| Utilities | $ 2,576 | $ 24,659 | $2,502,990 |
| Software and Technology Services | $ 1,252 | $ 103,838 | $7,258,233 |
| Healthcare | $ 4,409 | $ 49,875 | $ 583,153 |
| Financial Services | $ 4,637 | $ 88,298 | $5,798,573 |

**Average annual loss from data breach by segment (selected sectors)**

# THANK YOU

Questions and Answers

No part of this presentation may be copied or redistributed without the prior written consent of Guidewire. This material was used exclusively as an exhibit to an oral presentation. It may not be, nor should it be relied, upon as reflecting a complete record of the discussion.