Cyber data analytics

CAS Ratemaking and Product Management Seminar

13 March 2013

Ernst & Young

Quality In Everything We Do

Disclaimer

Ernst & Young refers to the global organization of member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited located in the US.

The views expressed by presenter(s) are not necessarily those of Ernst & Young LLP.

These slides are for educational purposes only and are not intended, and should not be relied upon, as accounting advice.

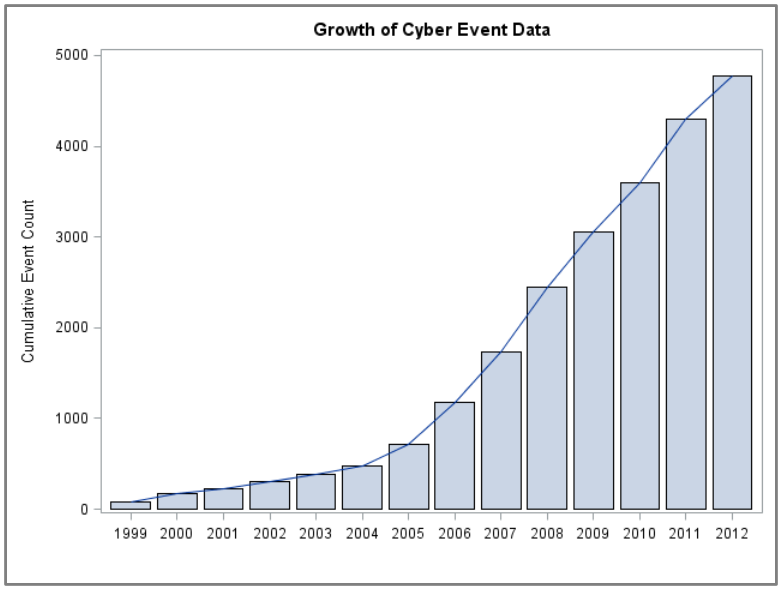
All charts and graphs are created by Ernst & Young LLP, to be used only by Ernst & Young LLP.

Agenda

- Cyber insurance considerations – current state
- Cyber data research
- Findings and observations
- Further ideas and applications

Cyber insurance considerations – current state

- Size of historical premium and loss information
- Qualitative rather than quantitative review of policy application
- Growth of cyber event data due to reporting guidelines
- Pricing considerations
  - Revenue
  - Employee count
  - IT security
  - Prior breaches
  - Coverage limits

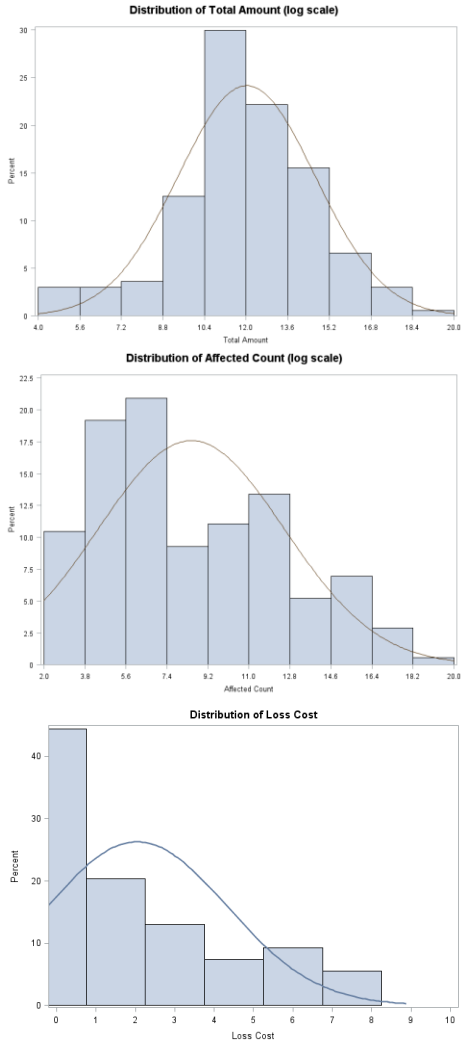


Cyber data research

- Goals from reviewing cyber event data
  - Determine the feasibility of a severity model that estimates ultimate cyber event cost
  - Find exposure bases which correlate well with frequency and severity
- Create ways to incorporate more rigor into the cyber insurance risk evaluation process by leveraging available cyber event data

Findings and observations – severity

- Focus on severity of cyber events
- Potential **response variables**
  - Total Damage Amount associated with event (combined 1st and 3rd party)
  - **Number of Affected Customers**
  - Loss Cost per customer (damages divided by affected customers)
- Types of randomness seen in the responses appear reasonable for applying predictive models



Findings and observations – severity

Dynamic financial data

- Debt
- Assets
- Fortune rank
- Share price
- Sales
- Employees
- Financial ratios
- Market cap

Static company information

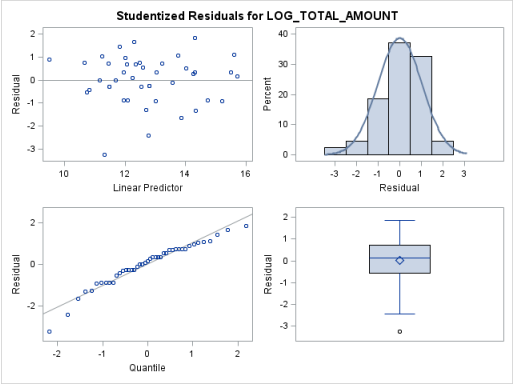
- Ownership type
- Location
- Industry

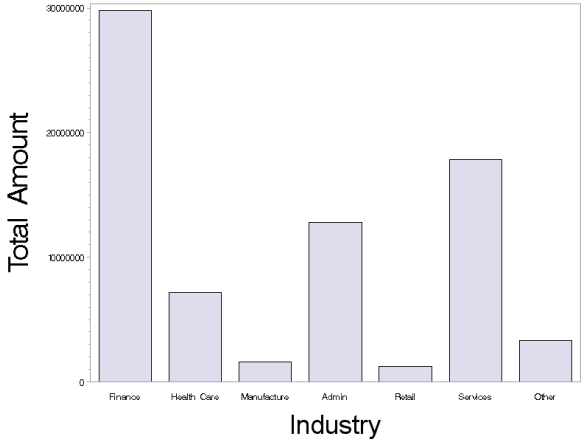
Event information

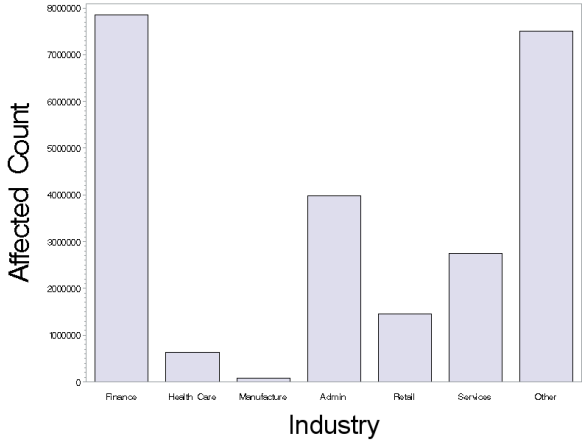
- Affected number of customers
- Credit card numbers
- Social security numbers
- External breach
- Hacking
- System failure
- Physical theft

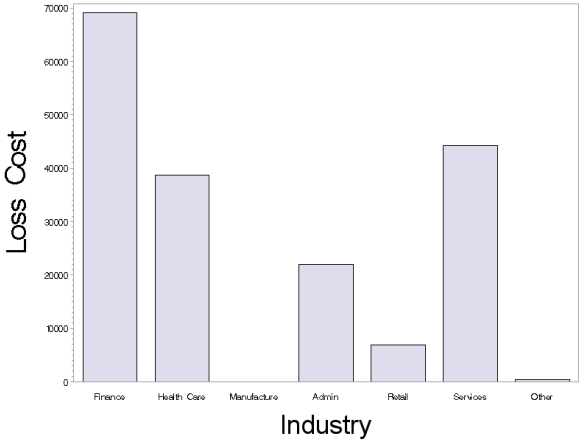
Findings and observations – severity

- Damage amount follows a typical loss distribution pattern
- Affected count is heavily skewed by large events
- Loss cost is sensitive to the size of event
  - Apply capping to avoid affect of outliers
  - Loss cost ranges from $0.50 to $10.00 per affected count depending on capping thresholds
- Pattern of the response variable varies noticeably across industries







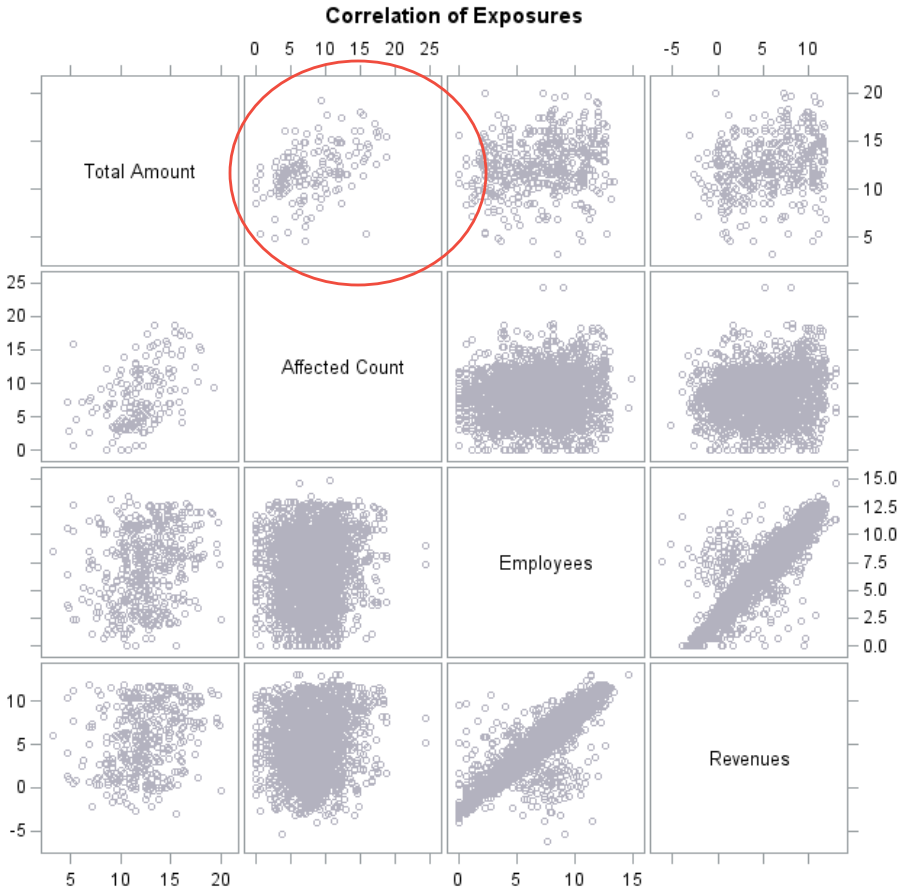


Findings and observations – severity

- Three facets of customer count
  - Affected count as a predictor of loss amount
  - Affected count as response for event severity
  - At time of underwriting a cyber policy, use customer count as an exposure basis for data breach coverage
- Two step model idea
  - Estimate the affected customer count of an event
  - Apply the result from step one as an input to estimate total damage amount

Findings and observations – exposure

- **Affected Customer Count** shows a significantly higher correlation with total amount than employee count or revenue



Findings and observations – frequency

- Create a basis pool of companies and append cyber event indicators for frequency analysis
- Public company data is more extensive and readily available than government or private company data
  - Approximately 35,000 public companies
  - Time series financial data
  - D&B information
  - SEC reporting guidelines for cyber events
    - *"The federal securities laws, in part, are designed to elicit disclosure of timely, comprehensive, and accurate information about risks and events that a reasonable investor would consider important to an investment decision..."*

Findings and observations – frequency

Potential **response variables**

- Annual event indicator
  - Binary: 0 for no event and 1 for one or more events in a given year
  - Estimate likelihood of at least one cyber attack over 12 months
- Number of events over a given time horizon
  - Estimate the number of cyber events over x months

Findings and observations – frequency

Dynamic financial data

- Debt
- Assets
- Fortune rank
- Share price
- Sales
- Employees
- Financial ratios
- Market cap

Static company information

- Ownership type
- Location
- Industry

Other (potential) company information

- Prior events
- Brand reputation
- Web presence
- Controversial products
- Political profile
- Public image
- Activist activities
- Data storage media
- IT security process/rating
- System access points

Further ideas and applications

- Consider refined measures of exposure
  - Customer count
  - Type of customer data (SSN, credit card, email)
  - Multi-peril nature of cyber policies
  - Multiple exposure bases by coverage and industry type
- Compare cyber insurance losses with actual and modeled event cost
- Simulate historical insured loss amounts for a given cyber insurance program structure
- Consider cyber cat and contagion risk, both of which are currently largely unquantified

Further ideas and applications

- Cyber insurance data collection and maintenance
  - Identify relevant event and claims information from available sources
  - Organize data to facilitate analytics
- Cyber insurance product design
  - Pricing considerations / rating elements
  - Reserving considerations
  - Underwriting guidelines
  - Derive parameters for new cyber coverage offerings