External Auditors' Assessments of Cyber-Security Risks

Tran Nguen Bao Ngo

VN-UK Institute for Research and Executive Education

University of Danang

Danang, Vietnam

tran.ngo@vnuk.edu.vn

Andrea Tick

Institute of Enterprise Management

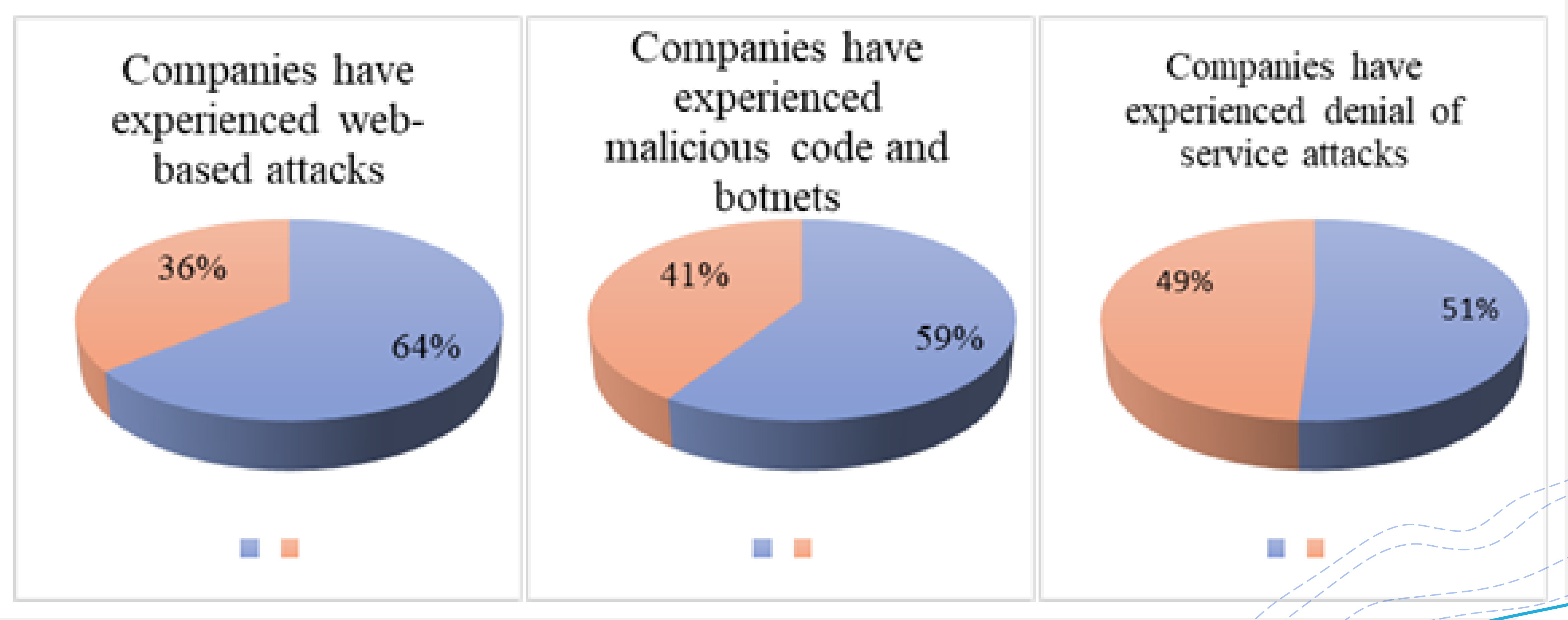
Keleti Faculty of Business and Management, Óbuda University

Budapest, Hungary

tick.andrea@kgk.uni-obuda.hu

Cybercriminals in business world

- 64% of companies have experiences web-based attacks
- 62% experiences phising & scial engineerng attacks
- 59% of companies experiences malicious code and botnest
- 51% experiences denial of service attacks



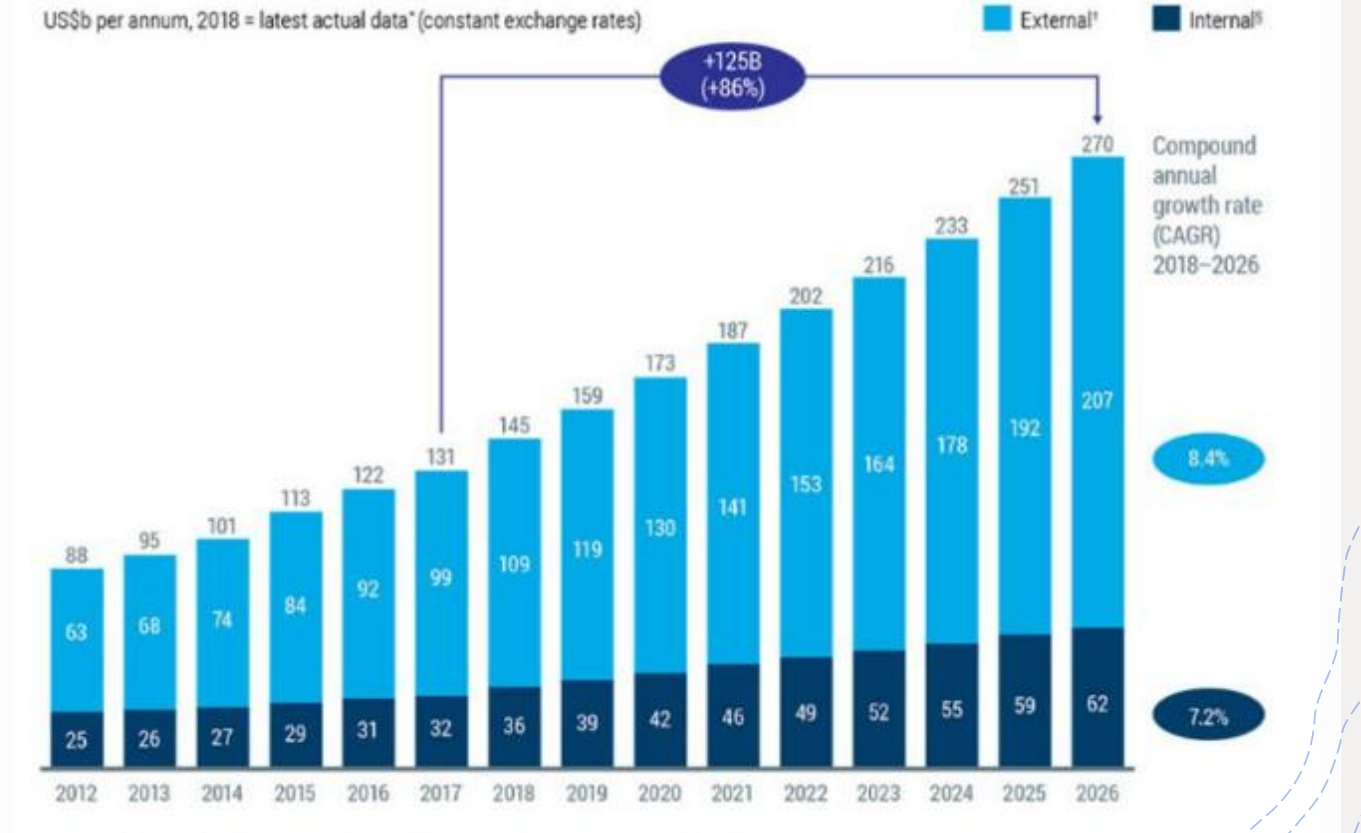
Companies have experienced web-based attacks

Companies have experienced malicious code and botnets

Companies have experienced denial of service attacks

Worldwide spending on information security products and services is increasing

- Worldwide spending on information security products and services will reach more than $114 billion in 2018, an increase of 12.4 percent from last year, according to the latest forecast from Gartner, Inc. In 2019, the market is forecast to grow 8.7 percent to $124 billion.



* 2012–2016 data based on Gartner data as at 3Q16; 2017 and beyond based on Gartner data

† External spend based on forecasts to 2023 provided by Gartner, extrapolated to 2026 using the average growth rates. Growth rates applied at the product segment level

§ Internal spend refers to the compensation of in-house full-time equivalent employees. Estimated based on Gartner data on global internal spending. Internal spend grows more slowly than external spend, linked to the increasing adoption of external managed security services

SOURCE: Gartner; Australian Bureau of Statistics; Burning Glass; expert interviews; AlphaBeta and McKinsey analysis

Cyber security and audit fee

- The most attention of the cybersecurity in business world focuses on the financial sector
  - financial information attack leads to a negative stock-market reaction,
  - a decline in sales growth for large firms and retail firms,
  - a rise in leverage,
  - a deterioration in financial health, and
  - a reduction in investment in the short run.

Cyber security and audit fee

auditors to pay more attention to cybersecurity-incident-occurring companies

1. it is the mission of external auditors to assess the client’s accounting for losses, claims, and liabilities related to a cyber-security incident once it happens in the context of a company finding difficult to cope with considerable and unexpected direct and indirect cost
2. in case of direct cyber-attacks to a company’s accounting system, external auditors are required to take into consideration the Internal Control over Financial Reporting (ICFR) because the incident could involve in the risk of the company’ accounting record manipulation, which results in the less trustful financial statements

Cyber security and audit fee

- As external auditors are put under enormous pressure when auditing cybersecurity-incident-occurring companies, it is necessary to discover how external auditors responds to cybersecurity incidents, and one of the common indicator is audit fee charges.

H_1: The cybersecurity incidents have positive impact on the high audit fees.

Methodology and data

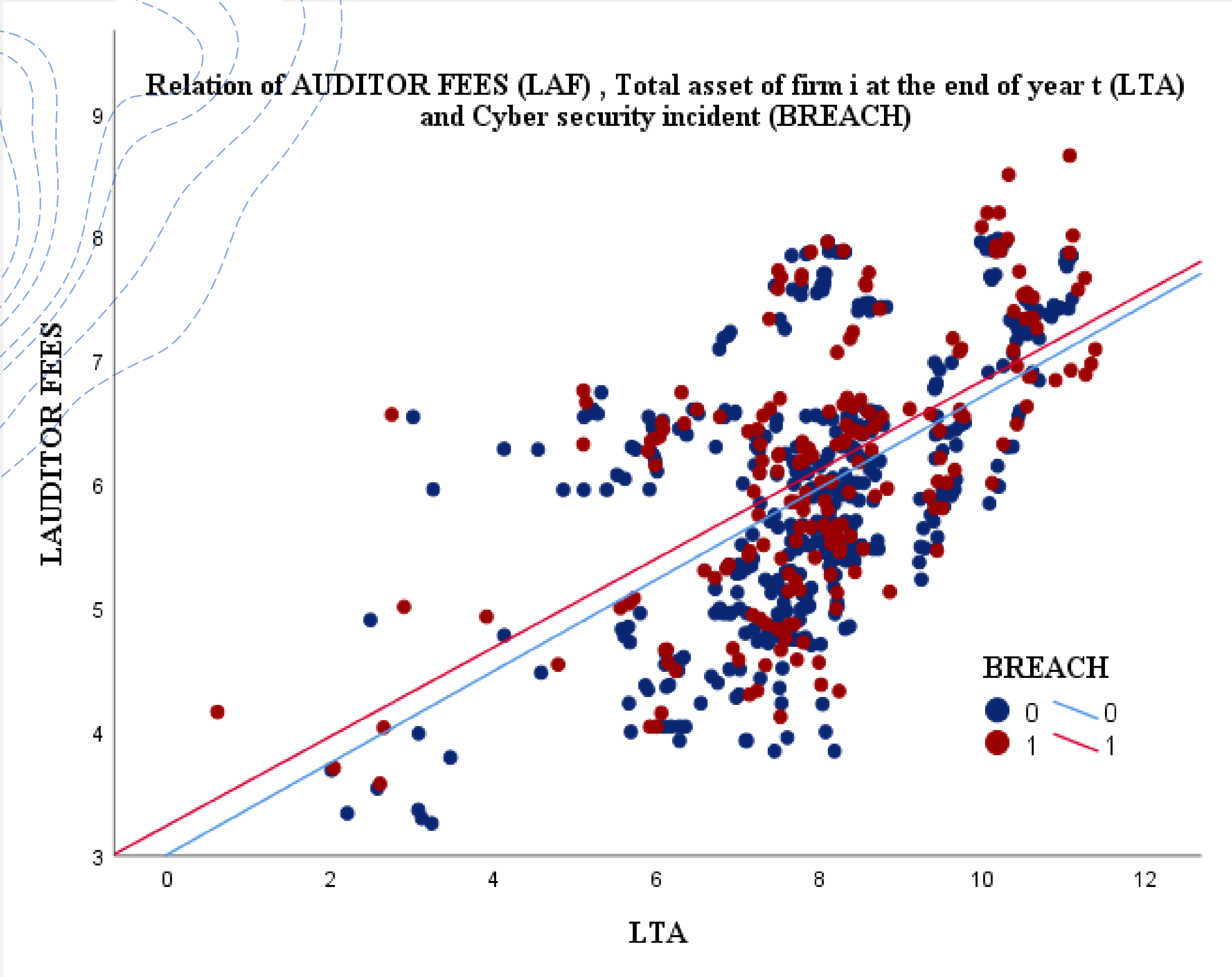
- 78 out of 100 worldwide firms listed Wharton Research Data Service
- small, medium and big companies with diverse major throughout the world
- the companies breach information is collected from Data Breaches shared by Privacy Rights Clearinghouse
- Quantitative method using the Ordinary Least Square (OLS) method
- Limitations:
  - Short period of time
  - Some missing financial data
  - Some insignificant controlling variables

The model

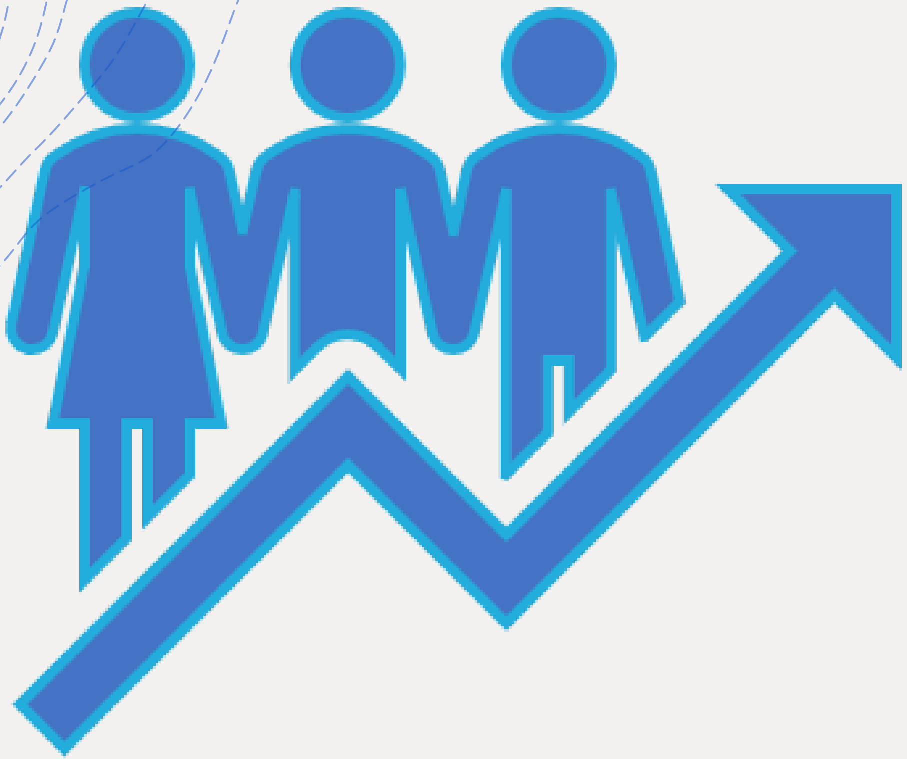
$$LAF_{i,t} = \beta_0 + \beta_1 BREACH + \beta_2 LTA + \beta_3 LLEV + \beta_4 CUR + \beta_5 QUICK + \beta_6 ROA + \beta_7\, DEBTEQ + \varepsilon_{i,t}\ \mathrm{A}$$

where:

- $LAF_{i,t}$ = logarithm of audit fees of firm i in year t, a proxy for the external auditors concern for cyber security risks;
- BREACH = 1 if a firm experiences a cyber-security incident in year t, 0 otherwise;
- LTA = logarithm of end of year total assets of firm i in year t;
- LLEV = logarithm of the ratio (current liabilities divided by total assets) of firm i in year t;
- CUR = the ratio (current assets divided by total assets) of firm i in year t;
- QUICK = difference between current assets and inventory divided by current liabilities of firm i in year t;
- ROA = earnings before interest and taxes divided by total assets of firm i in year t;
- DEBTEQ = the ratio (total debt divided by equity book value) of firm i in year t.



Relation of LAF, LTE and BREACH



Findings

- Correlation is positive between breach and audit fee
- The coefficient of BREACH is significantly positive (0.148793) at 5% level of confidence (p-value=0.0364).
- It confirms the expectation (β1>0).
- The coefficient of BREACH estimated at 0.148973 means that with all other variables unchanged, the increase of one cybersecurity incident of 100 examined companies from 2006 to 2014 will lead to nearly 14.9% increase in the audit fees.

Cybersecurity and audit fees

- The result shows an evident fact about the positive relationship between the audit fees charge and cybersecurity incident.
- It means that companies that experience cybersecurity attacks have a tendency to tolerate higher audit fees charge.

Conclusion

- external auditors express more concern for cybersecurity-attacked companies
- it provides support for those regulations and laws related to the role of external auditors in the context of terrible cyber crimes

THANK YOU FOR YOUR ATTENTION!