Cyber Insurance

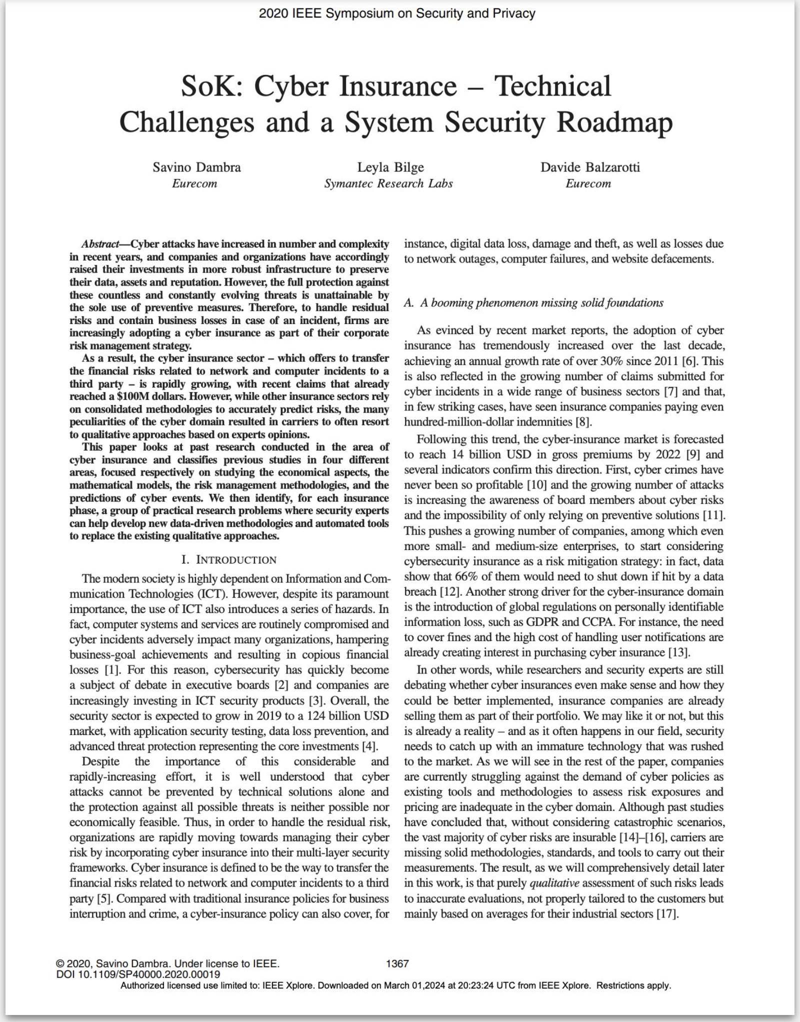
COMS6998 sec:12
Economics of Cybersecurity
5 March 2024

"An insurance salesman in an office, selling a cyber insurance policy to a concerned business executive"

Why are we talking about insurance in a computer science class?

- Accounts for billions of dollars of security spending

- Insurers see an aggregate picture of risk and are financially motivated to estimate it correctly (in theory)
    - Insurers are in a position to tell us which security investments are worth making (in theory)



2020 IEEE Symposium on Security and Privacy

SoK: Cyber Insurance – Technical Challenges and a System Security Roadmap

Savino Dambra
Eurecom

Leyla Bilge
Symantec Research Labs

Davide Balzarotti
Eurecom

***Abstract*—Cyber attacks have increased in number and complexity in recent years, and companies and organizations have accordingly raised their investments in more robust infrastructure to preserve their data, assets and reputation. However, the full protection against these countless and constantly evolving threats is unattainable by the sole use of preventive measures. Therefore, to handle residual risks and contain business losses in case of an incident, firms are increasingly adopting a cyber insurance as part of their corporate risk management strategy.**

As a result, the cyber insurance sector – which offers to transfer the financial risks related to network and computer incidents to a third party – is rapidly growing, with recent claims that already reached a $100M dollars. However, while other insurance sectors rely on consolidated methodologies to accurately predict risks, the many peculiarities of the cyber domain resulted in carriers to often resort to qualitative approaches based on experts opinions.

This paper looks at past research conducted in the area of cyber insurance and classifies previous studies in four different areas, focused respectively on studying the economical aspects, the mathematical models, the risk management methodologies, and the predictions of cyber events. We then identify, for each insurance phase, a group of practical research problems where security experts can help develop new data-driven methodologies and automated tools to replace the existing qualitative approaches.

I. Introduction

The modern society is highly dependent on Information and Communication Technologies (ICT). However, despite its paramount importance, the use of ICT also introduces a series of hazards. In fact, computer systems and services are routinely compromised and cyber incidents adversely impact many organizations, hampering business-goal achievements and resulting in copious financial losses [1]. For this reason, cybersecurity has quickly become a subject of debate in executive boards [2] and companies are increasingly investing in ICT security products [3]. Overall, the security sector is expected to grow in 2019 to a 124 billion USD market, with application security testing, data loss prevention, and advanced threat protection representing the core investments [4].

Despite the importance of this considerable and rapidly-increasing effort, it is well understood that cyber attacks cannot be prevented by technical solutions alone and the protection against all possible threats is neither possible nor economically feasible. Thus, in order to handle the residual risk, organizations are rapidly moving towards managing their cyber risk by incorporating cyber insurance into their multi-layer security frameworks. Cyber insurance is defined to be the way to transfer the financial risks related to network and computer incidents to a third party [5]. Compared with traditional insurance policies for business interruption and crime, a cyber-insurance policy can also cover, for instance, digital data loss, damage and theft, as well as losses due to network outages, computer failures, and website defacements.

A. A booming phenomenon missing solid foundations

As evinced by recent market reports, the adoption of cyber insurance has tremendously increased over the last decade, achieving an annual growth rate of over 30% since 2011 [6]. This is also reflected in the growing number of claims submitted for cyber incidents in a wide range of business sectors [7] and that, in few striking cases, have seen insurance companies paying even hundred-million-dollar indemnities [8].

Following this trend, the cyber-insurance market is forecasted to reach 14 billion USD in gross premiums by 2022 [9] and several indicators confirm this direction. First, cyber crimes have never been so profitable [10] and the growing number of attacks is increasing the awareness of board members about cyber risks and the impossibility of only relying on preventive solutions [11]. This pushes a growing number of companies, among which even more small- and medium-size enterprises, to start considering cybersecurity insurance as a risk mitigation strategy: in fact, data show that 66% of them would need to shut down if hit by a data breach [12]. Another strong driver for the cyber-insurance domain is the introduction of global regulations on personally identifiable information loss, such as GDPR and CCPA. For instance, the need to cover fines and the high cost of handling user notifications are already creating interest in purchasing cyber insurance [13].

In other words, while researchers and security experts are still debating whether cyber insurances even make sense and how they could be better implemented, insurance companies are already selling them as part of their portfolio. We may like it or not, but this is already a reality – and as it often happens in our field, security needs to catch up with an immature technology that was rushed to the market. As we will see in the rest of the paper, companies are currently struggling against the demand of cyber policies as existing tools and methodologies to assess risk exposures and pricing are inadequate in the cyber domain. Although past studies have concluded that, without considering catastrophic scenarios, the vast majority of cyber risks are insurable [14]–[16], carriers are missing solid methodologies, standards, and tools to carry out their measurements. The result, as we will comprehensively detail later in this work, is that purely *qualitative* assessment of such risks leads to inaccurate evaluations, not properly tailored to the customers but mainly based on averages for their industrial sectors [17].

DOI 10.1109/SP40000.2020.00019

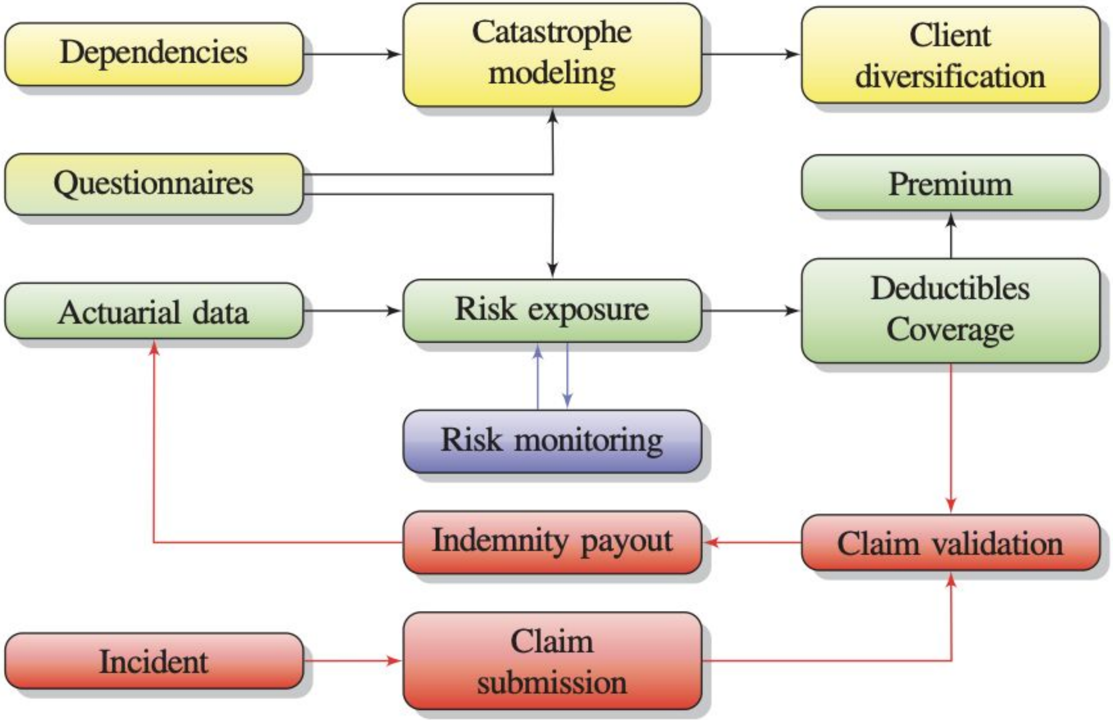


Fig. 1: Classic insurance process workflow extended in a cyber scenario (● Portfolio Management ● Underwriting ● Post binding ● Claiming)

Insurance basics + terminology

- **Insurer/Insurance company**: The party who sells insurance

https://www.insurance.ca.gov/01-consumers/105-type/95-guides/20-Glossary/

Insurance basics + terminology

- **Insurer/Insurance company**: The party who sells insurance
- **Insuree**/**insured/policyholder/claimant**: The party who buys insurance

https://www.insurance.ca.gov/01-consumers/105-type/95-guides/20-Glossary/

Insurance basics + terminology

- **Insurer/Insurance company**: The party who sells insurance
- **Insuree**/**insured/policyholder/claimant**: The party who buys insurance
- **Policy:** A contract between insurer and insuree specifying terms of insurance

https://www.insurance.ca.gov/01-consumers/105-type/95-guides/20-Glossary/

Insurance basics + terminology

- **Insurer/Insurance company**: The party who sells insurance
- **Insuree/insured/policyholder/claimant**: The party who buys insurance
- **Policy:** A contract between insurer and insuree specifying terms of insurance
  - **Premium**: The amount paid monthly/annually to keep the policy active

https://www.insurance.ca.gov/01-consumers/105-type/95-guides/20-Glossary/

Insurance basics + terminology

- **Insurer/Insurance company**: The party who sells insurance
- **Insuree**/**insured/policyholder/claimant**: The party who buys insurance
- **Policy:** A contract between insurer and insuree specifying terms of insurance
  - **Premium**: The amount paid monthly/annually to keep the policy active
  - **Retention**/**Deductible:** Amount that policyholder is liable for (even with policy)

https://www.insurance.ca.gov/01-consumers/105-type/95-guides/20-Glossary/

Insurance basics + terminology

- **Insurer/Insurance company**: The party who sells insurance
- **Insuree**/**insured/policyholder/claimant**: The party who buys insurance
- **Policy:** A contract between insurer and insuree specifying terms of insurance
  - **Premium**: The amount paid monthly/annually to keep the policy active
  - **Retention**/**Deductible:** Amount that policyholder is liable for (even with policy)
  - **Limit:** Maximum amount a policy will pay a policyholder

https://www.insurance.ca.gov/01-consumers/105-type/95-guides/20-Glossary/

Insurance basics + terminology

- **Insurer/Insurance company**: The party who sells insurance
- **Insuree/insured/policyholder/claimant**: The party who buys insurance
- **Policy:** A contract between insurer and insuree specifying terms of insurance
  - **Premium**: The amount paid monthly/annually to keep the policy active
  - **Retention/Deductible:** Amount that policyholder is liable for (even with policy)
  - **Limit:** Maximum amount a policy will pay a policyholder
  - **Exclusions:** Clauses and conditions that are not covered by the policy

https://www.insurance.ca.gov/01-consumers/105-type/95-guides/20-Glossary/

Insurance basics + terminology

- **Insurer/Insurance company**: The party who sells insurance
- **Insuree**/**insured/policyholder/claimant**: The party who buys insurance
- **Policy:** A contract between insurer and insuree specifying terms of insurance
  - **Premium**: The amount paid monthly/annually to keep the policy active
  - **Retention**/**Deductible:** Amount that policyholder is liable for (even with policy)
  - **Limit:** Maximum amount a policy will pay a policyholder
  - **Exclusions:** Clauses and conditions that are not covered by the policy
- **Underwriting**: The process of creating a policy

https://www.insurance.ca.gov/01-consumers/105-type/95-guides/20-Glossary/

Insurance basics + terminology

- **Claim**: A request by an policyholder to receive compensation for a covered loss

https://www.insurance.ca.gov/01-consumers/105-type/95-guides/20-Glossary/

Insurance basics + terminology

- **Claim**: A request by an policyholder to receive compensation for a covered loss
    - **First-Party Losses**: Financial harms incurred by the policyholder

https://www.insurance.ca.gov/01-consumers/105-type/95-guides/20-Glossary/

Insurance basics + terminology

- **Claim**: A request by an policyholder to receive compensation for a covered loss
  - **First-Party Losses**: Financial harms incurred by the policyholder
  - **Third-Party Losses**: Financial harms incurred parties other than policyholder

https://www.insurance.ca.gov/01-consumers/105-type/95-guides/20-Glossary/

Insurance basics + terminology

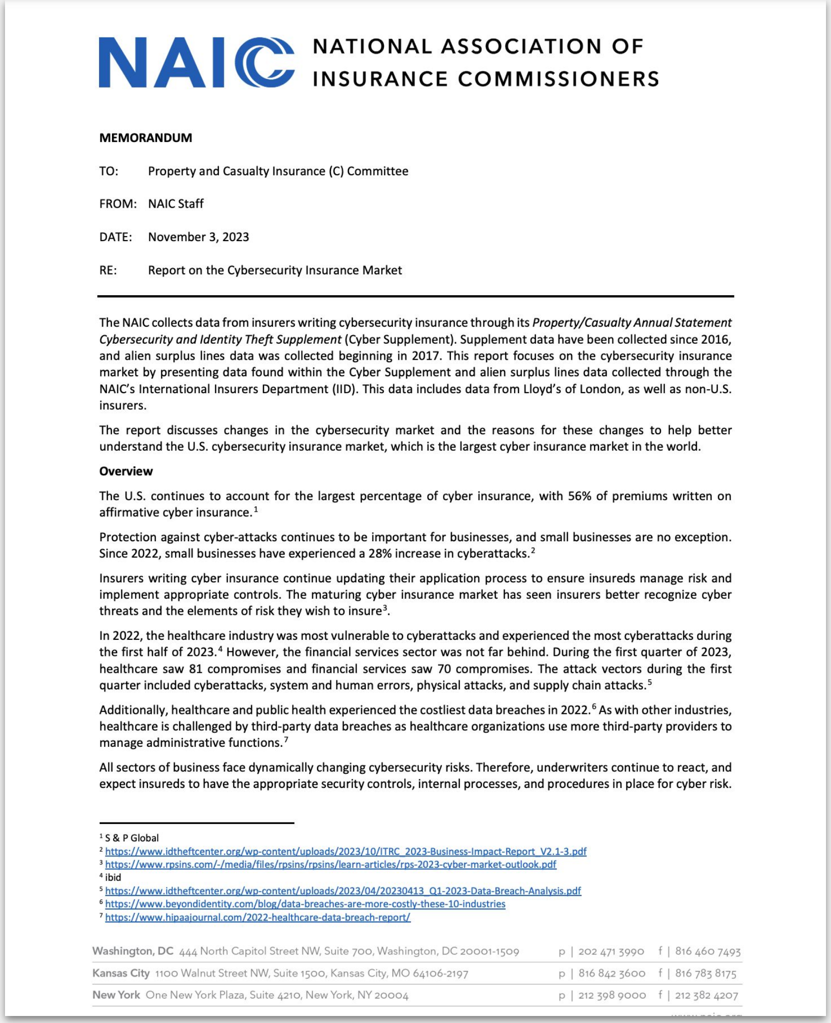
- **Claim**: A request by an policyholder to receive compensation for a covered loss
  - **First-Party Losses**: Financial harms incurred by the policyholder
  - **Third-Party Losses**: Financial harms incurred parties other than policyholder
- **Diversification:** A strategy for avoiding catastrophic losses by covering many different types of policyholders with independent probabilities of losses

https://www.insurance.ca.gov/01-consumers/105-type/95-guides/20-Glossary/

What are some of the challenges facing cyber insurance?

What are some of the challenges facing cyber insurance?

1. Asymmetric information leads to adverse selection
2. Risk estimation is difficult due to interdependent nature of tech
3. Not enough actuarial information to accurately price risk
   a. Many incidents go unreported to save reputation
   b. Threats are constantly adapting and evolving
4. Tech monocultures prevent diversification
5. Market lacks reinsurers
6. Post-binding phase drives up costs
7. Harms can be intangible and hard to precisely quantify



NAIC NATIONAL ASSOCIATION OF
INSURANCE COMMISSIONERS

MEMORANDUM

TO: Property and Casualty Insurance (C) Committee

FROM: NAIC Staff

DATE: November 3, 2023

RE: Report on the Cybersecurity Insurance Market

The NAIC collects data from insurers writing cybersecurity insurance through its *Property/Casualty Annual Statement Cybersecurity and Identity Theft Supplement* (Cyber Supplement). Supplement data have been collected since 2016, and alien surplus lines data was collected beginning in 2017. This report focuses on the cybersecurity insurance market by presenting data found within the Cyber Supplement and alien surplus lines data collected through the NAIC's International Insurers Department (IID). This data includes data from Lloyd's of London, as well as non-U.S. insurers.

The report discusses changes in the cybersecurity market and the reasons for these changes to help better understand the U.S. cybersecurity insurance market, which is the largest cyber insurance market in the world.

Overview

The U.S. continues to account for the largest percentage of cyber insurance, with 56% of premiums written on affirmative cyber insurance.[1]

Protection against cyber-attacks continues to be important for businesses, and small businesses are no exception. Since 2022, small businesses have experienced a 28% increase in cyberattacks.[2]

Insurers writing cyber insurance continue updating their application process to ensure insureds manage risk and implement appropriate controls. The maturing cyber insurance market has seen insurers better recognize cyber threats and the elements of risk they wish to insure[3].

In 2022, the healthcare industry was most vulnerable to cyberattacks and experienced the most cyberattacks during the first half of 2023.[4] However, the financial services sector was not far behind. During the first quarter of 2023, healthcare saw 81 compromises and financial services saw 70 compromises. The attack vectors during the first quarter included cyberattacks, system and human errors, physical attacks, and supply chain attacks.[5]

Additionally, healthcare and public health experienced the costliest data breaches in 2022.[6] As with other industries, healthcare is challenged by third-party data breaches as healthcare organizations use more third-party providers to manage administrative functions.[7]

All sectors of business face dynamically changing cybersecurity risks. Therefore, underwriters continue to react, and expect insureds to have the appropriate security controls, internal processes, and procedures in place for cyber risk.

[1] S & P Global
[2] https://www.idtheftcenter.org/wp-content/uploads/2023/10/ITRC_2023-Business-Impact-Report_V2.1-3.pdf
[3] https://www.rpsins.com/-/media/files/rpsins/rpsins/learn-articles/rps-2023-cyber-market-outlook.pdf
[4] ibid
[5] https://www.idtheftcenter.org/wp-content/uploads/2023/04/20230413_Q1-2023-Data-Breach-Analysis.pdf
[6] https://www.beyondidentity.com/blog/data-breaches-are-more-costly-these-10-industries
[7] https://www.hipaajournal.com/2022-healthcare-data-breach-report/

How much is spent on cyber insurance each year?

A. $1M
B. $10M
C. $100M
D. $1B
E. $10B

How much is spent on cyber insurance each year?

A. $1M

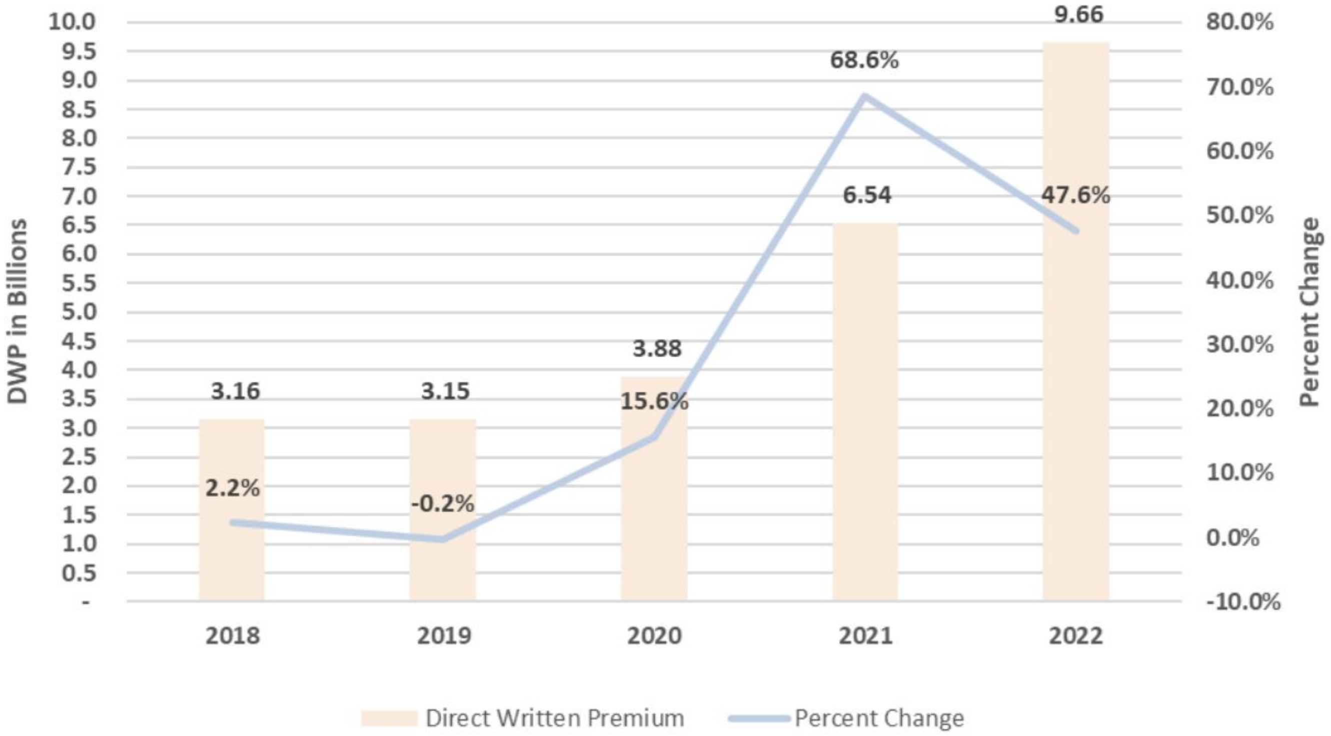
B. $10M

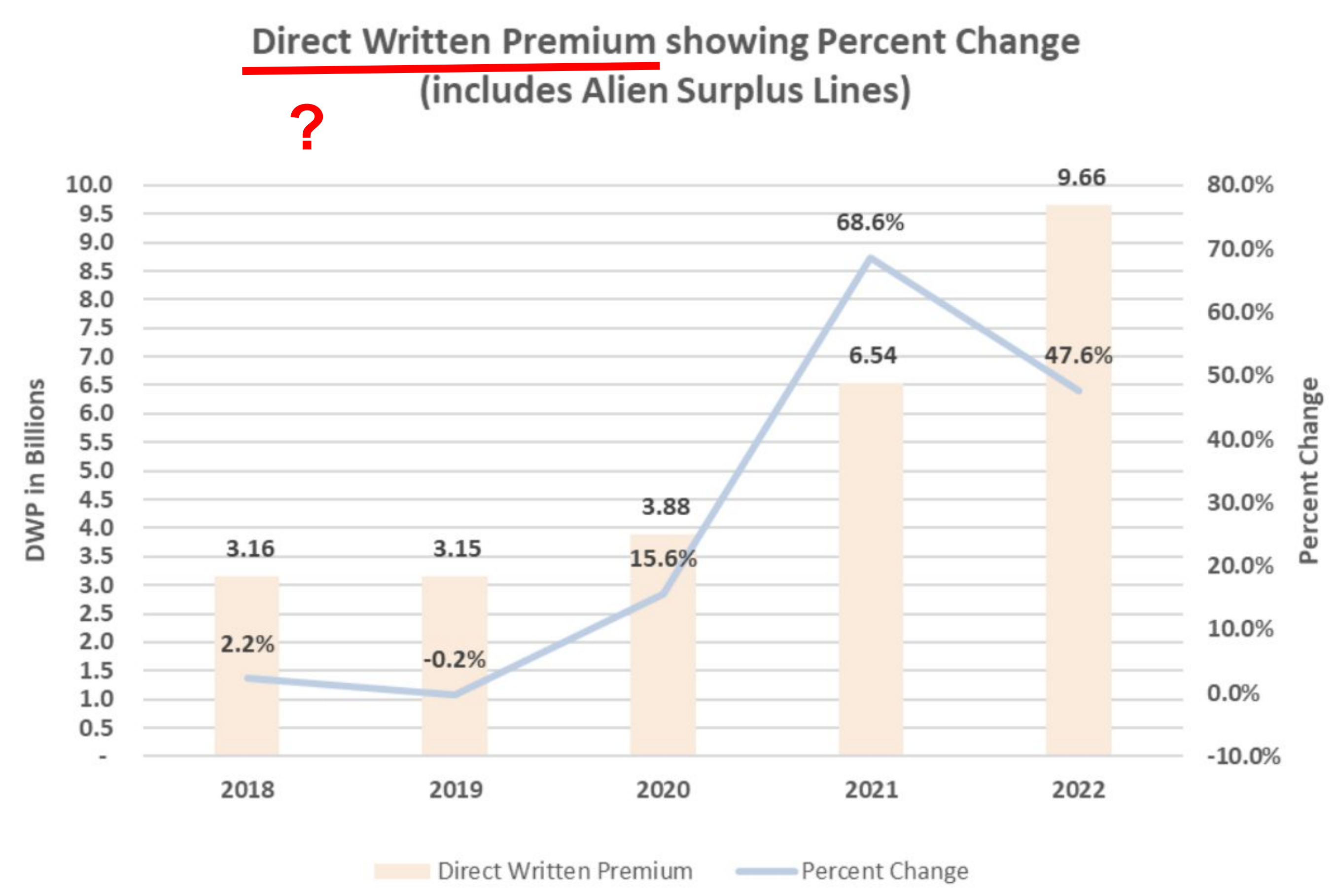
C. $100M

D. $1B

[✓ E. $10B]

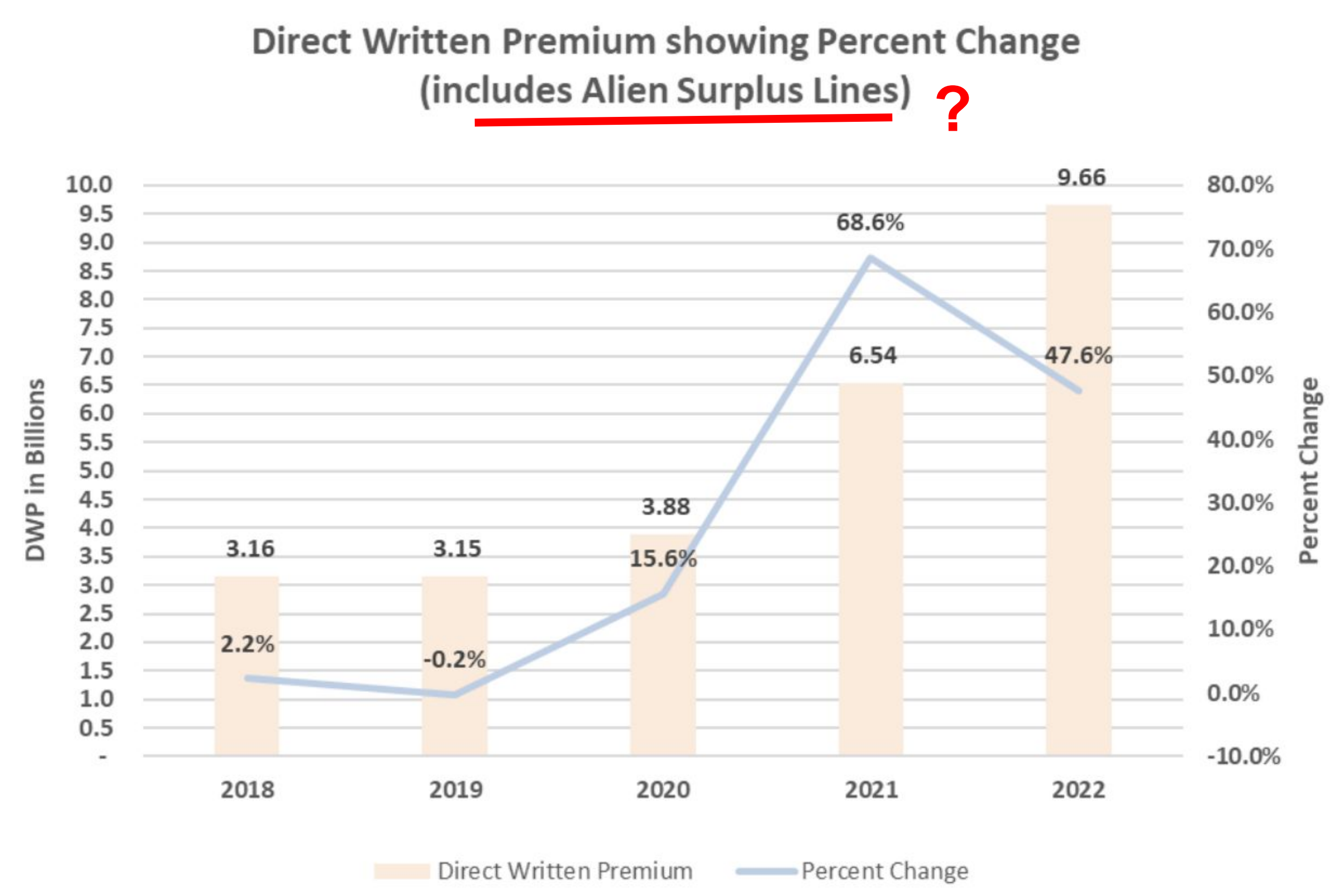
Direct Written Premium showing Percent Change (includes Alien Surplus Lines)



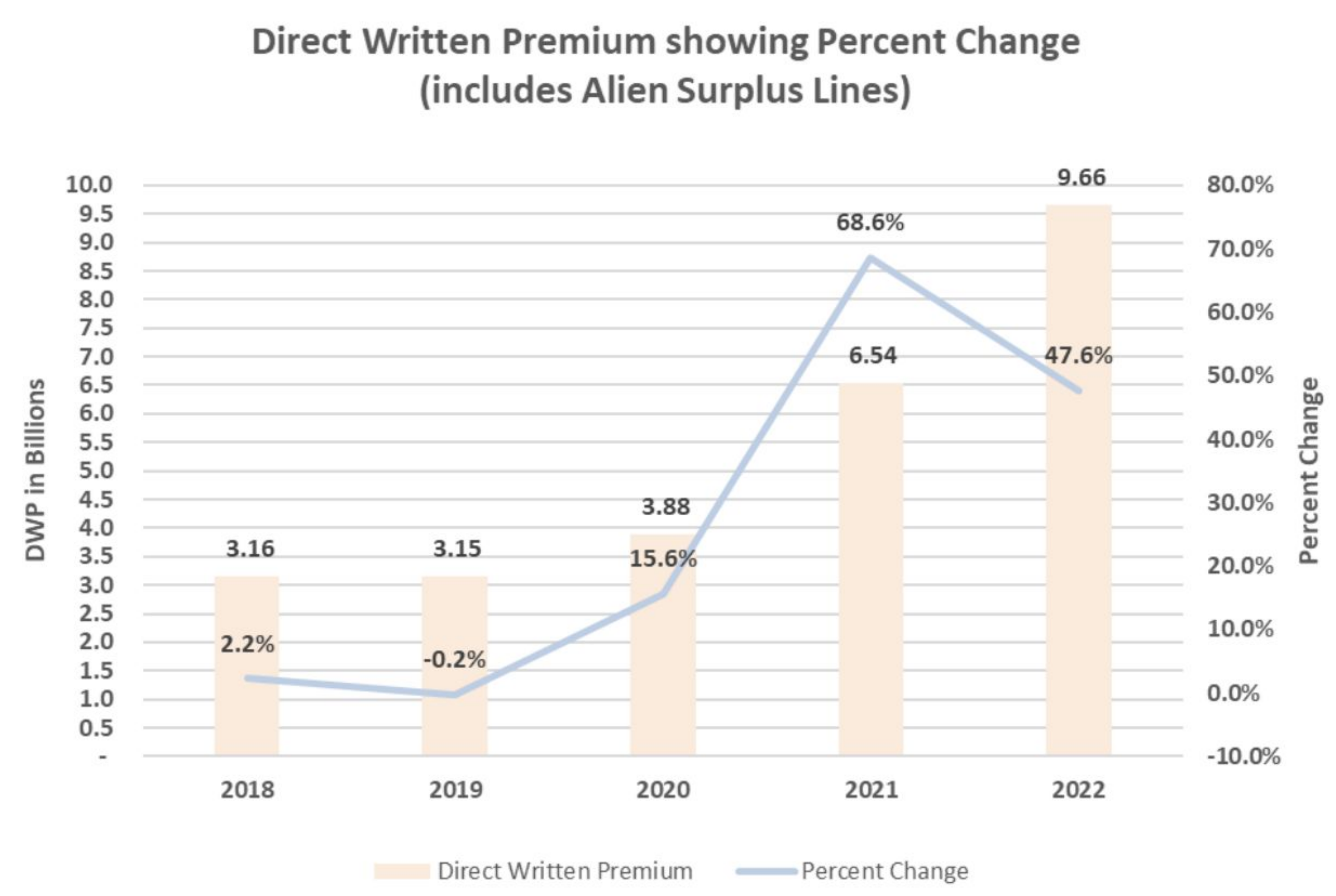


Direct Written Premium showing Percent Change
(includes Alien Surplus Lines)

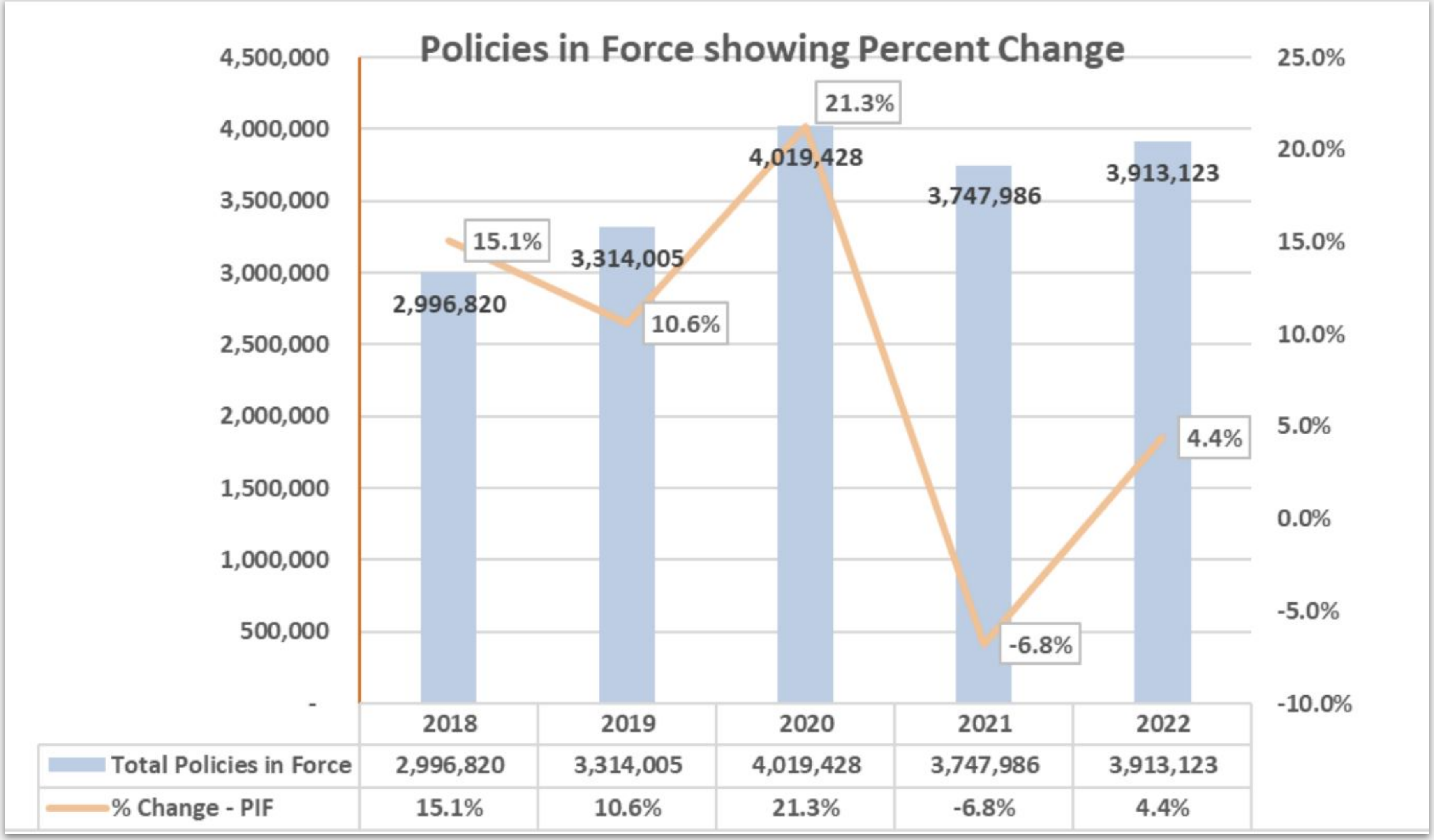
?



Direct Written Premium showing Percent Change (includes Alien Surplus Lines) ?



Direct Written Premium showing Percent Change (includes Alien Surplus Lines)



Policies in Force showing Percent Change

	2018	2019	2020	2021	2022
▬ Total Policies in Force	2,996,820	3,314,005	4,019,428	3,747,986	3,913,123
▬ % Change - PIF	15.1%	10.6%	21.3%	-6.8%	4.4%

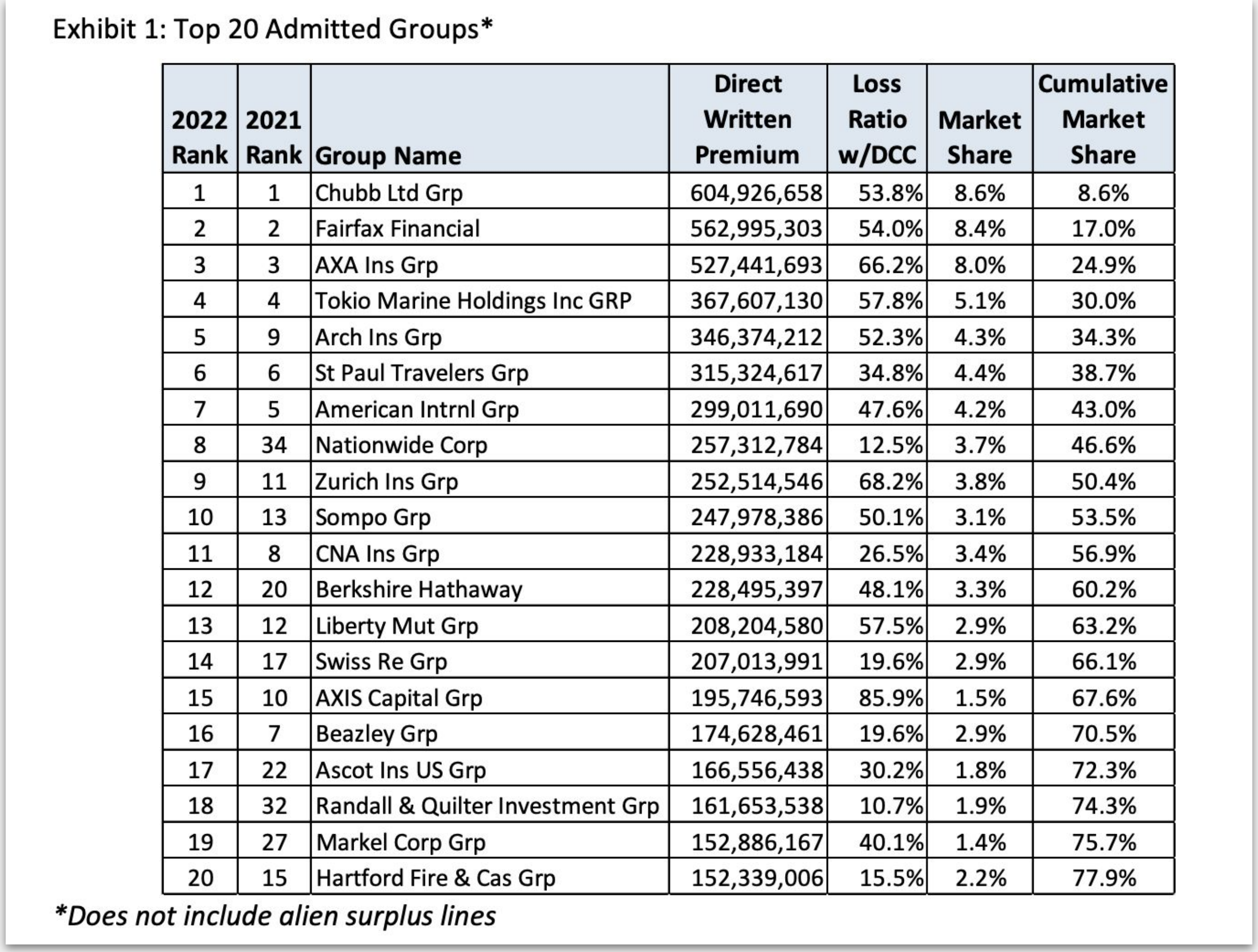
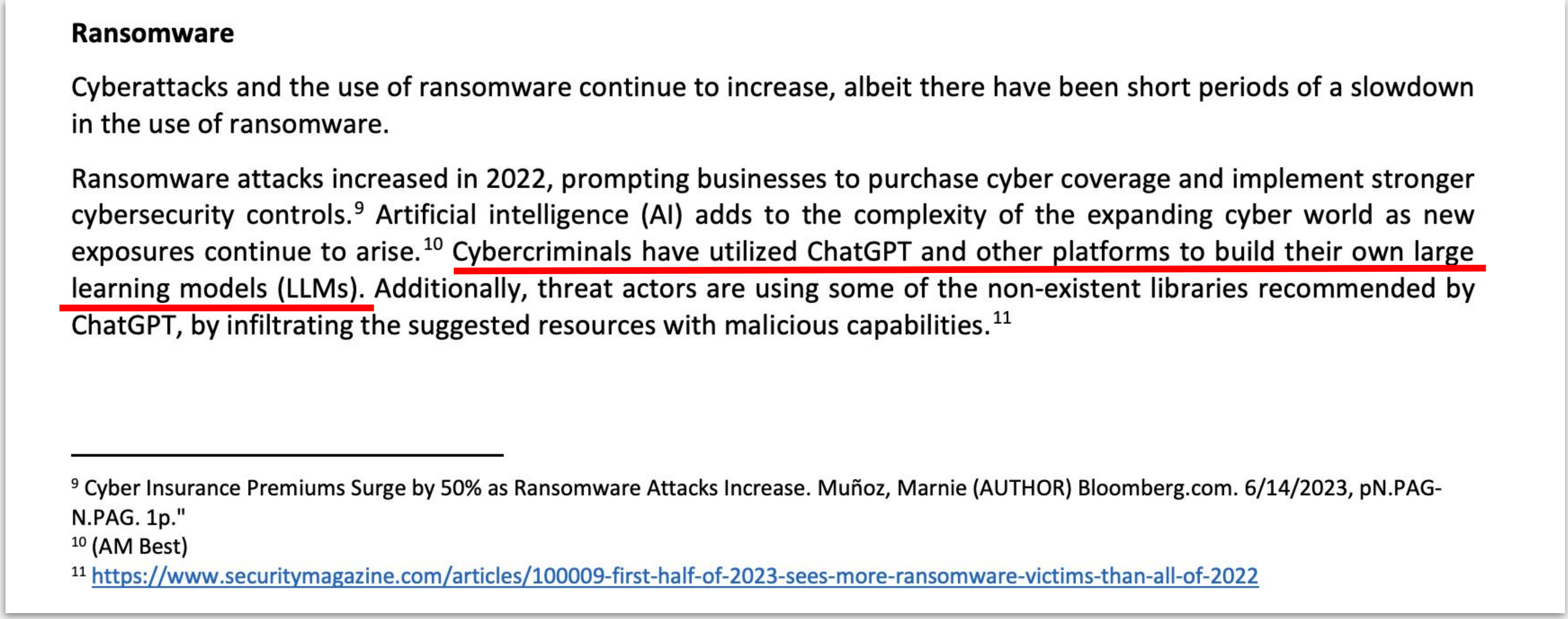


Exhibit 1: Top 20 Admitted Groups*

2022 Rank	2021 Rank	Group Name	Direct Written Premium	Loss Ratio w/DCC	Market Share	Cumulative Market Share
1	1	Chubb Ltd Grp	604,926,658	53.8%	8.6%	8.6%
2	2	Fairfax Financial	562,995,303	54.0%	8.4%	17.0%
3	3	AXA Ins Grp	527,441,693	66.2%	8.0%	24.9%
4	4	Tokio Marine Holdings Inc GRP	367,607,130	57.8%	5.1%	30.0%
5	9	Arch Ins Grp	346,374,212	52.3%	4.3%	34.3%
6	6	St Paul Travelers Grp	315,324,617	34.8%	4.4%	38.7%
7	5	American Intrnl Grp	299,011,690	47.6%	4.2%	43.0%
8	34	Nationwide Corp	257,312,784	12.5%	3.7%	46.6%
9	11	Zurich Ins Grp	252,514,546	68.2%	3.8%	50.4%
10	13	Sompo Grp	247,978,386	50.1%	3.1%	53.5%
11	8	CNA Ins Grp	228,933,184	26.5%	3.4%	56.9%
12	20	Berkshire Hathaway	228,495,397	48.1%	3.3%	60.2%
13	12	Liberty Mut Grp	208,204,580	57.5%	2.9%	63.2%
14	17	Swiss Re Grp	207,013,991	19.6%	2.9%	66.1%
15	10	AXIS Capital Grp	195,746,593	85.9%	1.5%	67.6%
16	7	Beazley Grp	174,628,461	19.6%	2.9%	70.5%
17	22	Ascot Ins US Grp	166,556,438	30.2%	1.8%	72.3%
18	32	Randall & Quilter Investment Grp	161,653,538	10.7%	1.9%	74.3%
19	27	Markel Corp Grp	152,886,167	40.1%	1.4%	75.7%
20	15	Hartford Fire & Cas Grp	152,339,006	15.5%	2.2%	77.9%

**Does not include alien surplus lines*



Ransomware

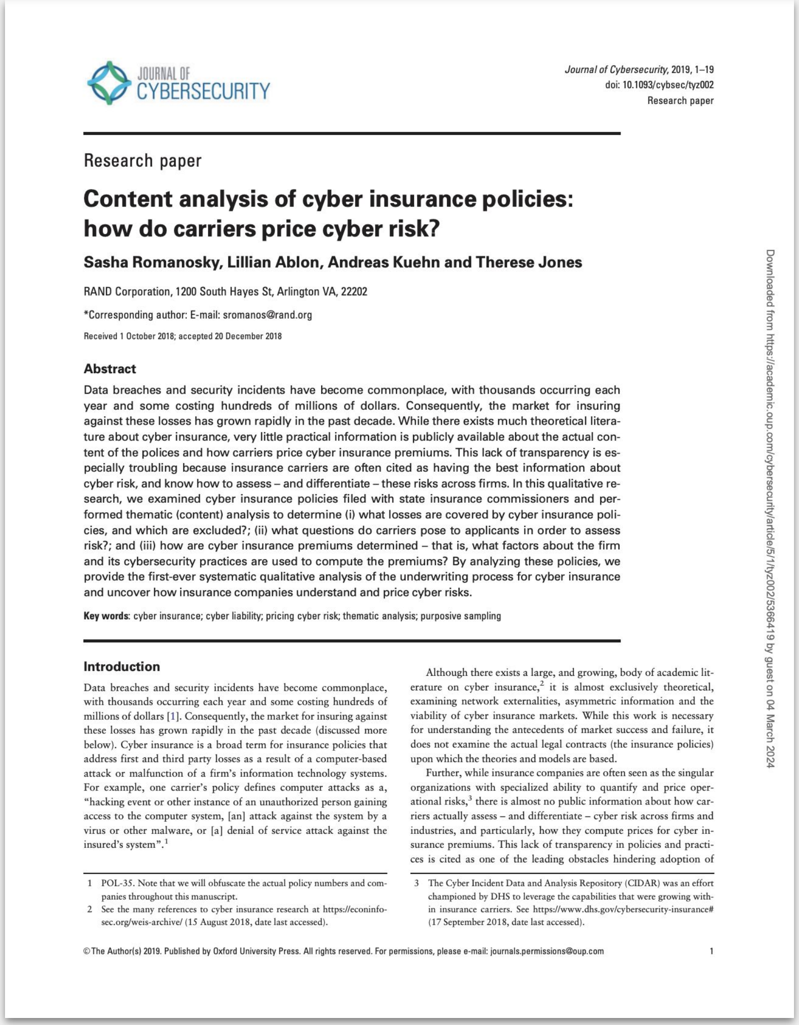
Cyberattacks and the use of ransomware continue to increase, albeit there have been short periods of a slowdown in the use of ransomware.

Ransomware attacks increased in 2022, prompting businesses to purchase cyber coverage and implement stronger cybersecurity controls.[9] Artificial intelligence (AI) adds to the complexity of the expanding cyber world as new exposures continue to arise.[10] Cybercriminals have utilized ChatGPT and other platforms to build their own large learning models (LLMs). Additionally, threat actors are using some of the non-existent libraries recommended by ChatGPT, by infiltrating the suggested resources with malicious capabilities.[11]

[9] Cyber Insurance Premiums Surge by 50% as Ransomware Attacks Increase. Muñoz, Marnie (AUTHOR) Bloomberg.com. 6/14/2023, pN.PAG-N.PAG. 1p."

[10] (AM Best)

[11] https://www.securitymagazine.com/articles/100009-first-half-of-2023-sees-more-ransomware-victims-than-all-of-2022



JOURNAL OF CYBERSECURITY

Journal of Cybersecurity, 2019, 1–19
doi: 10.1093/cybsec/tyz002
Research paper

Research paper

Content analysis of cyber insurance policies: how do carriers price cyber risk?

Sasha Romanosky, Lillian Ablon, Andreas Kuehn and Therese Jones

RAND Corporation, 1200 South Hayes St, Arlington VA, 22202

*Corresponding author: E-mail: sromanos@rand.org

Received 1 October 2018; accepted 20 December 2018

Abstract

Data breaches and security incidents have become commonplace, with thousands occurring each year and some costing hundreds of millions of dollars. Consequently, the market for insuring against these losses has grown rapidly in the past decade. While there exists much theoretical literature about cyber insurance, very little practical information is publicly available about the actual content of the polices and how carriers price cyber insurance premiums. This lack of transparency is especially troubling because insurance carriers are often cited as having the best information about cyber risk, and know how to assess – and differentiate – these risks across firms. In this qualitative research, we examined cyber insurance policies filed with state insurance commissioners and performed thematic (content) analysis to determine (i) what losses are covered by cyber insurance policies, and which are excluded?; (ii) what questions do carriers pose to applicants in order to assess risk?; and (iii) how are cyber insurance premiums determined – that is, what factors about the firm and its cybersecurity practices are used to compute the premiums? By analyzing these policies, we provide the first-ever systematic qualitative analysis of the underwriting process for cyber insurance and uncover how insurance companies understand and price cyber risks.

Key words: cyber insurance; cyber liability; pricing cyber risk; thematic analysis; purposive sampling

Introduction

Data breaches and security incidents have become commonplace, with thousands occurring each year and some costing hundreds of millions of dollars [1]. Consequently, the market for insuring against these losses has grown rapidly in the past decade (discussed more below). Cyber insurance is a broad term for insurance policies that address first and third party losses as a result of a computer-based attack or malfunction of a firm's information technology systems. For example, one carrier's policy defines computer attacks as a, "hacking event or other instance of an unauthorized person gaining access to the computer system, [an] attack against the system by a virus or other malware, or [a] denial of service attack against the insured's system".[1]

Although there exists a large, and growing, body of academic literature on cyber insurance,[2] it is almost exclusively theoretical, examining network externalities, asymmetric information and the viability of cyber insurance markets. While this work is necessary for understanding the antecedents of market success and failure, it does not examine the actual legal contracts (the insurance policies) upon which the theories and models are based.

Further, while insurance companies are often seen as the singular organizations with specialized ability to quantify and price operational risks,[3] there is almost no public information about how carriers actually assess – and differentiate – cyber risk across firms and industries, and particularly, how they compute prices for cyber insurance premiums. This lack of transparency in policies and practices is cited as one of the leading obstacles hindering adoption of

[1] POL-35. Note that we will obfuscate the actual policy numbers and companies throughout this manuscript.

[2] See the many references to cyber insurance research at https://econinfosec.org/weis-archive/ (15 August 2018, date last accessed).

[3] The Cyber Incident Data and Analysis Repository (CIDAR) was an effort championed by DHS to leverage the capabilities that were growing within insurance carriers. See https://www.dhs.gov/cybersecurity-insurance# (17 September 2018, date last accessed).

How was the data acquired?

A. Publicly available records
B. Interviewing insurance companies
C. Interviewing insurance policyholders
D. Posing as a company and submitting fake requests to insurance companies for insurance policies

How was the data acquired?

[✓ A. Publicly available records]

B. Interviewing insurance companies

C. Interviewing insurance policyholders

D. Posing as a company and submitting fake requests to insurance companies for insurance policies

How did the authors determine the number of policies to analyze?

A. Thematic analysis
B. Semi-random election
C. Inductive exhaustion
D. Ranked sampling

How did the authors determine the number of policies to analyze?

[✓ A. Thematic analysis]

B. Semi-random election

C. Inductive exhaustion

D. Ranked sampling

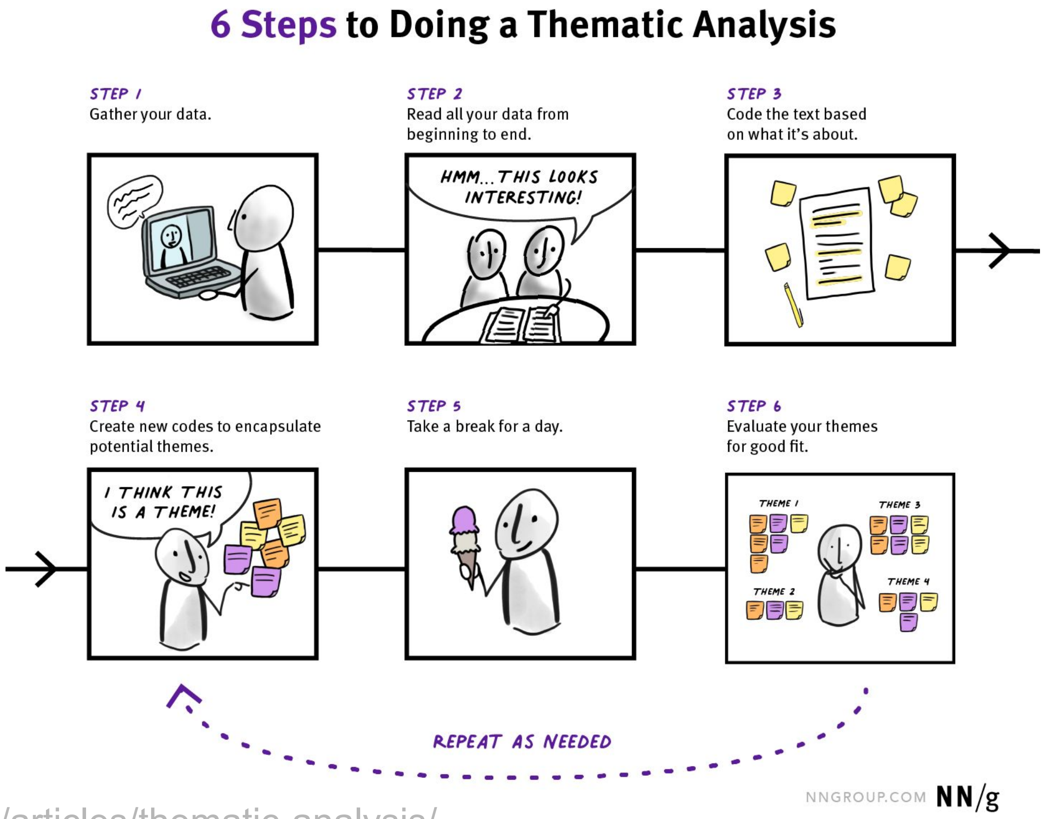
Aside on qualitative research

Imagine you have a large amount of unstructured text (via documents/interviews/etc.)

There are themes and patterns in the text but you don’t know what they are

1. How can you rigorously find important takeaways in the data?
2. How can you quantify trends in qualitative data?

Aside on qualitative research



6 Steps to Doing a Thematic Analysis

STEP 1
Gather your data.

STEP 2
Read all your data from beginning to end.

STEP 3
Code the text based on what it's about.

STEP 4
Create new codes to encapsulate potential themes.

STEP 5
Take a break for a day.

STEP 6
Evaluate your themes for good fit.

NNGROUP.COM NN/g

https://www.nngroup.com/articles/thematic-analysis/

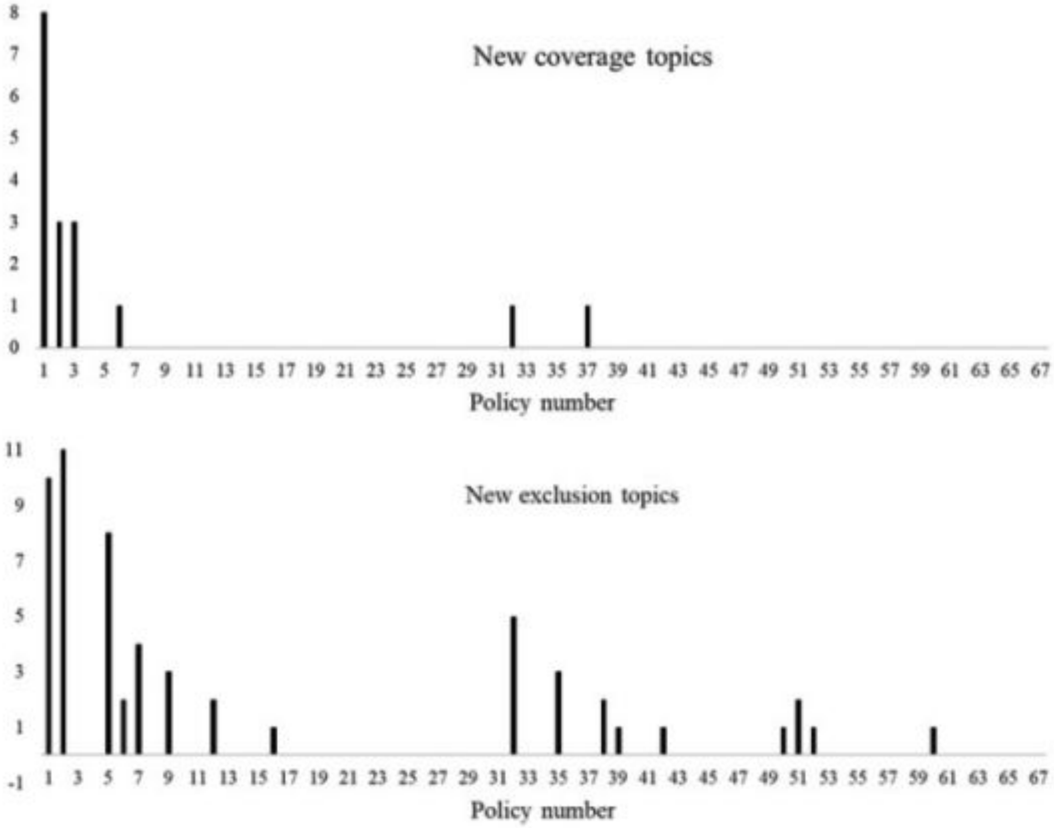


Figure 1: Identification of criteria over the course of reviewing policies

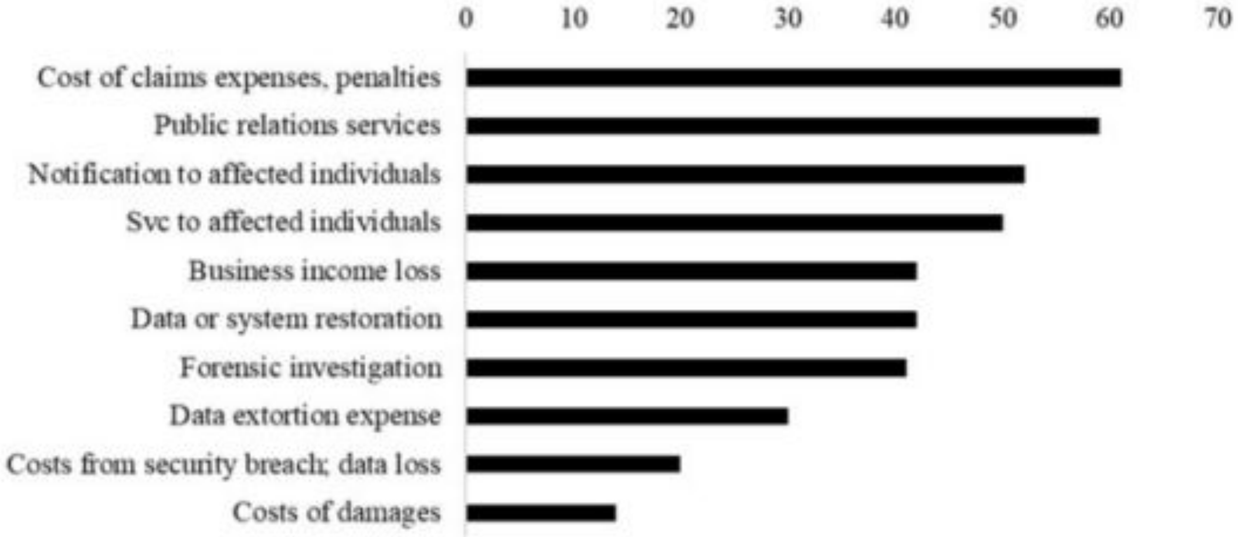


Figure 2: Most common covered losses

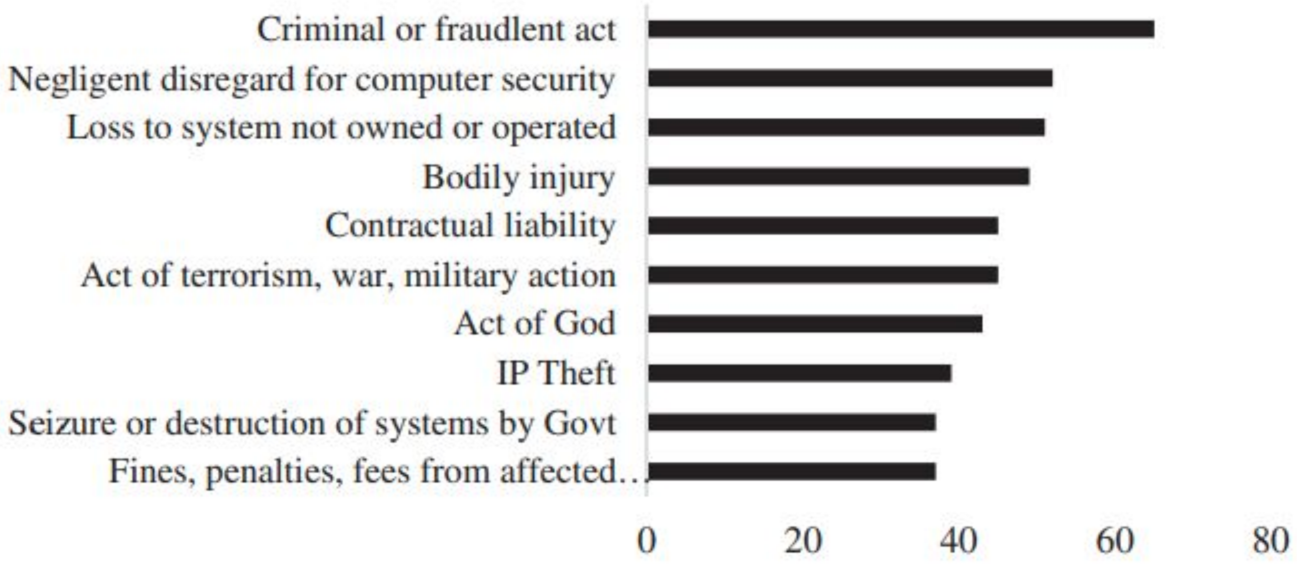


Figure 3: Most common exclusions

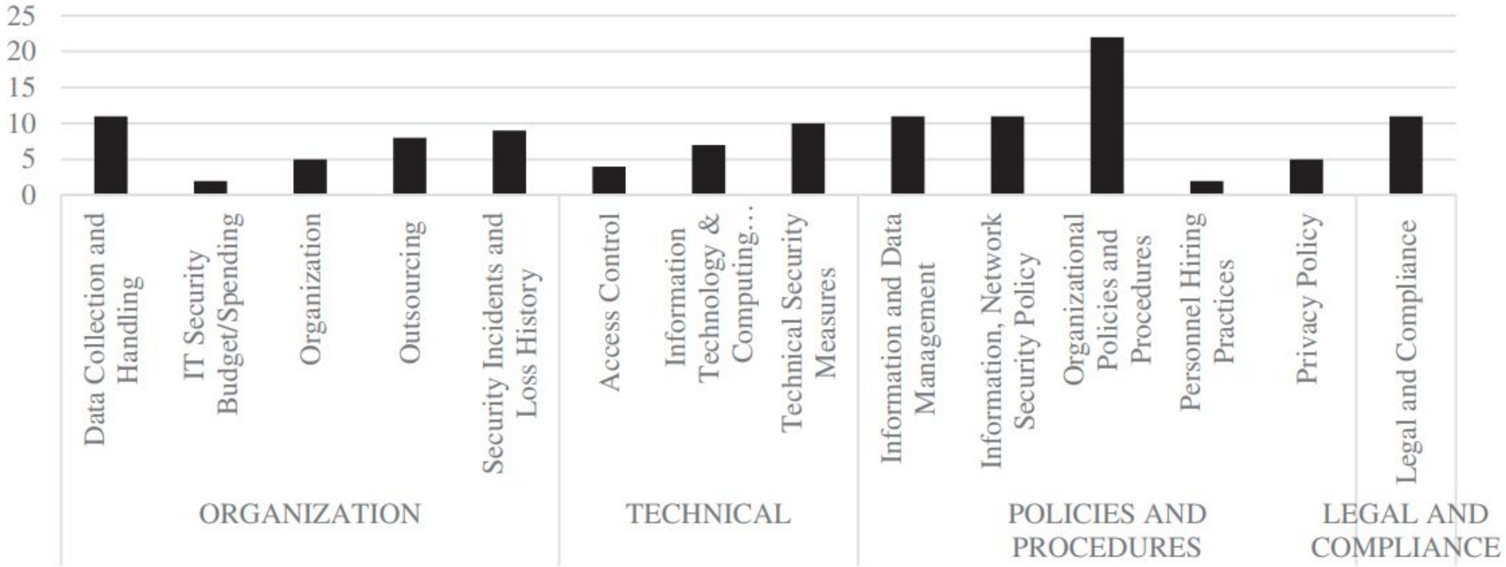


Figure 4: Number of unique questions per subcategory

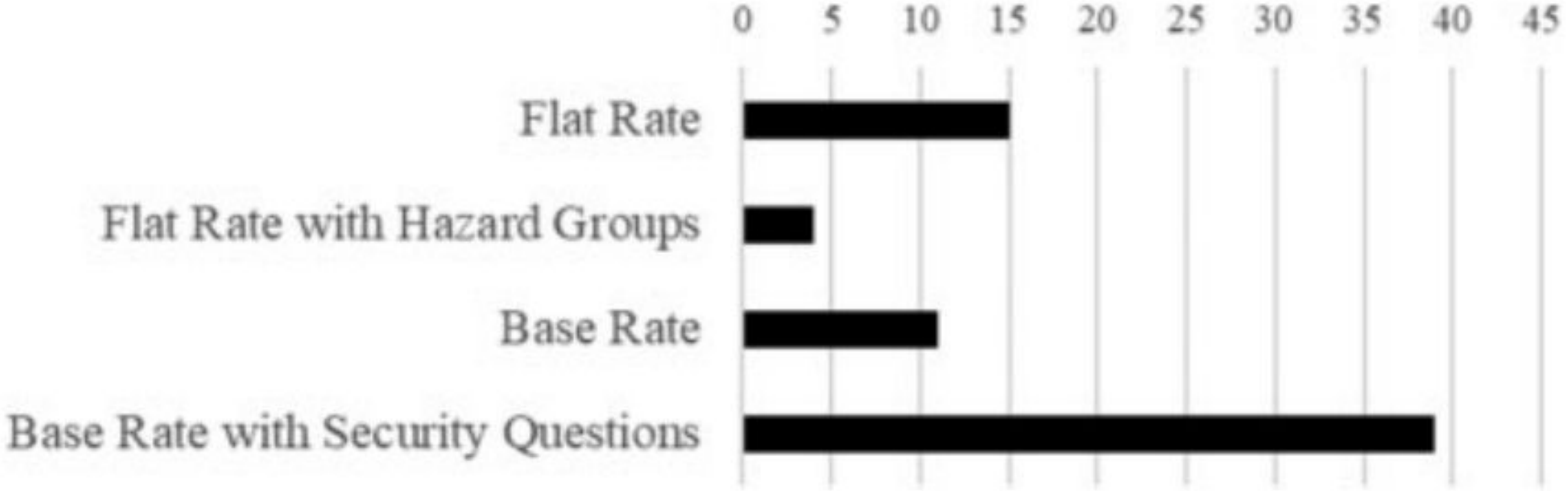


Figure 6: Rate schedule categories (*n* = 69)

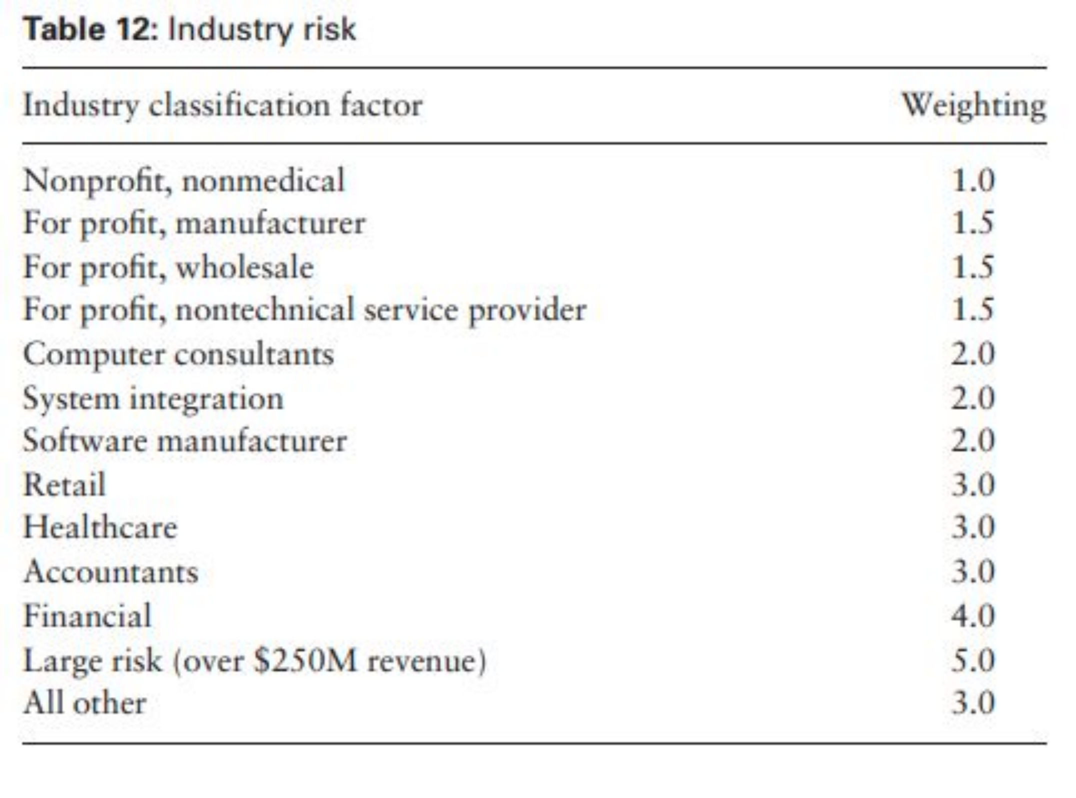


Table 12: Industry risk

Industry classification factor	Weighting
Nonprofit, nonmedical	1.0
For profit, manufacturer	1.5
For profit, wholesale	1.5
For profit, nontechnical service provider	1.5
Computer consultants	2.0
System integration	2.0
Software manufacturer	2.0
Retail	3.0
Healthcare	3.0
Accountants	3.0
Financial	4.0
Large risk (over $250M revenue)	5.0
All other	3.0

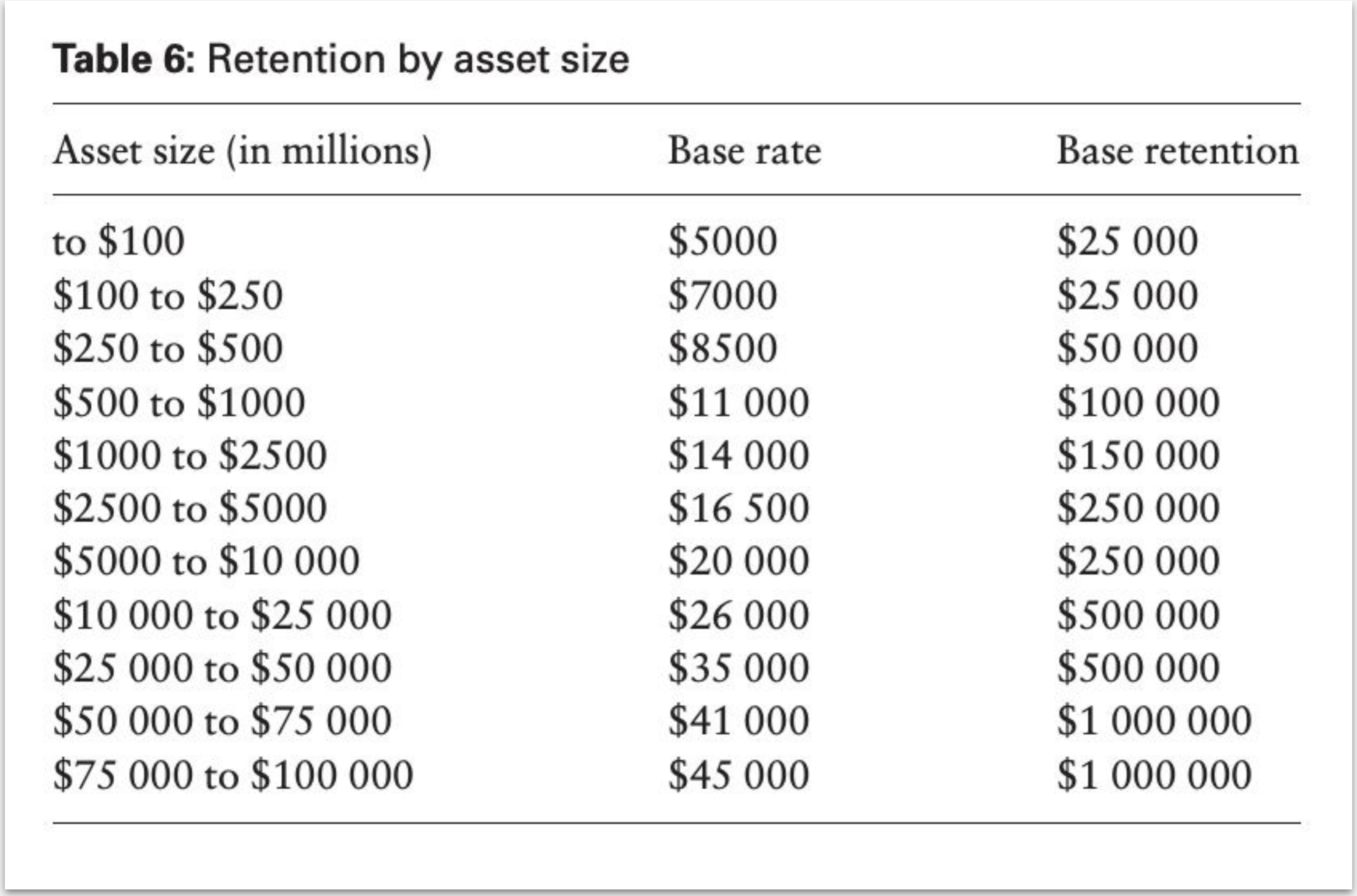


Table 6: Retention by asset size

Asset size (in millions)	Base rate	Base retention
to $100	$5000	$25 000
$100 to $250	$7000	$25 000
$250 to $500	$8500	$50 000
$500 to $1000	$11 000	$100 000
$1000 to $2500	$14 000	$150 000
$2500 to $5000	$16 500	$250 000
$5000 to $10 000	$20 000	$250 000
$10 000 to $25 000	$26 000	$500 000
$25 000 to $50 000	$35 000	$500 000
$50 000 to $75 000	$41 000	$1 000 000
$75 000 to $100 000	$45 000	$1 000 000

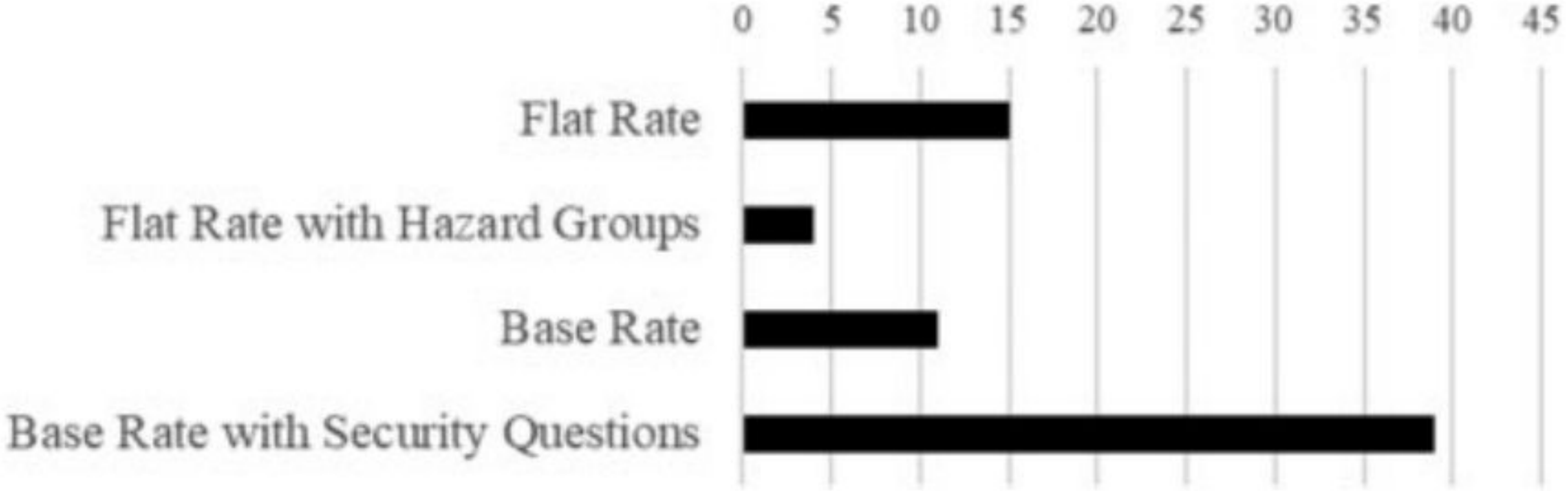


Figure 6: Rate schedule categories (*n* = 69)

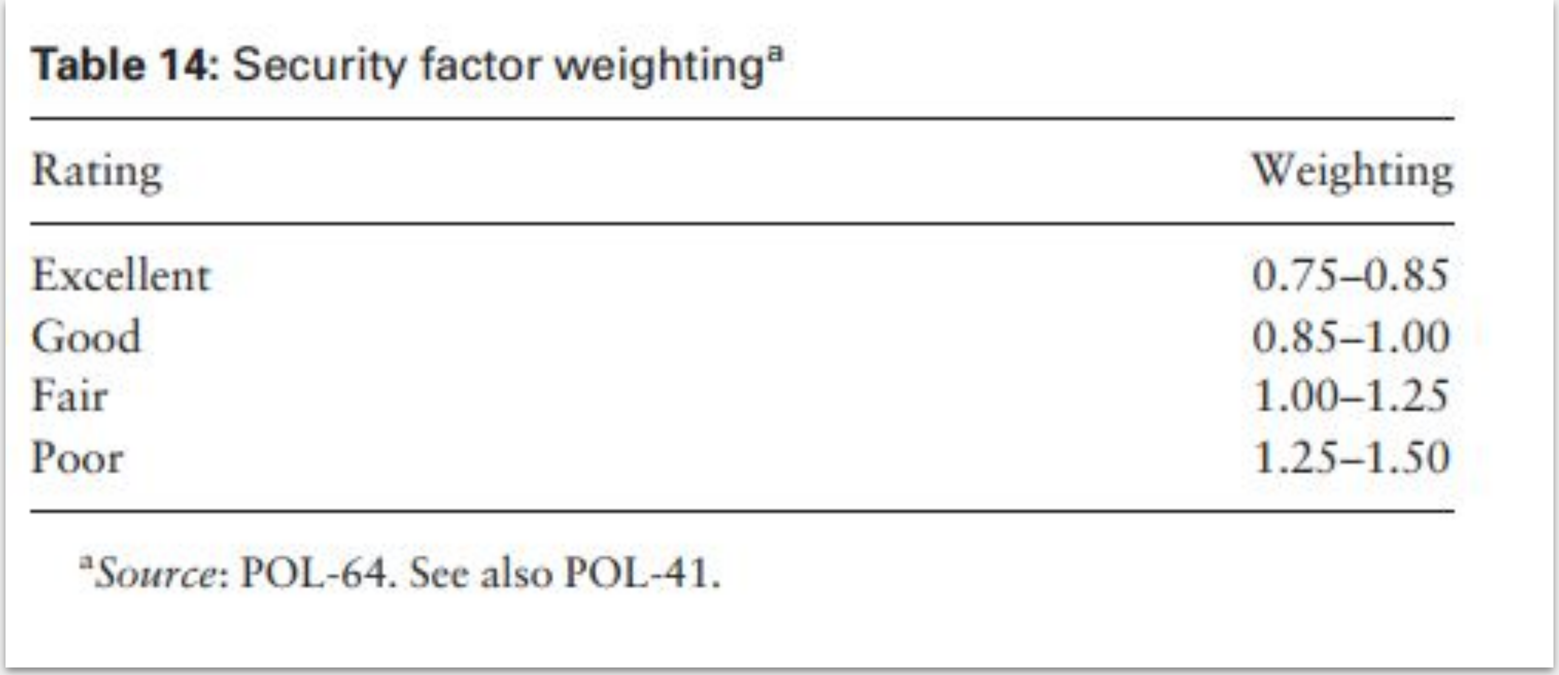
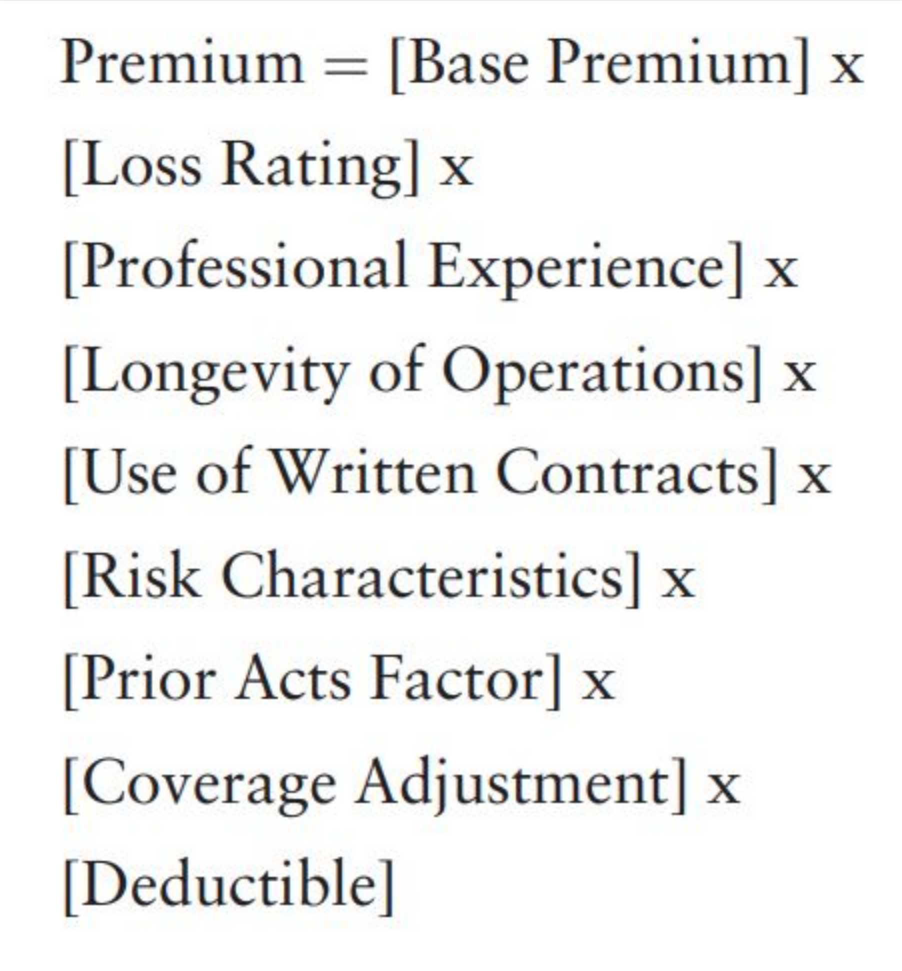


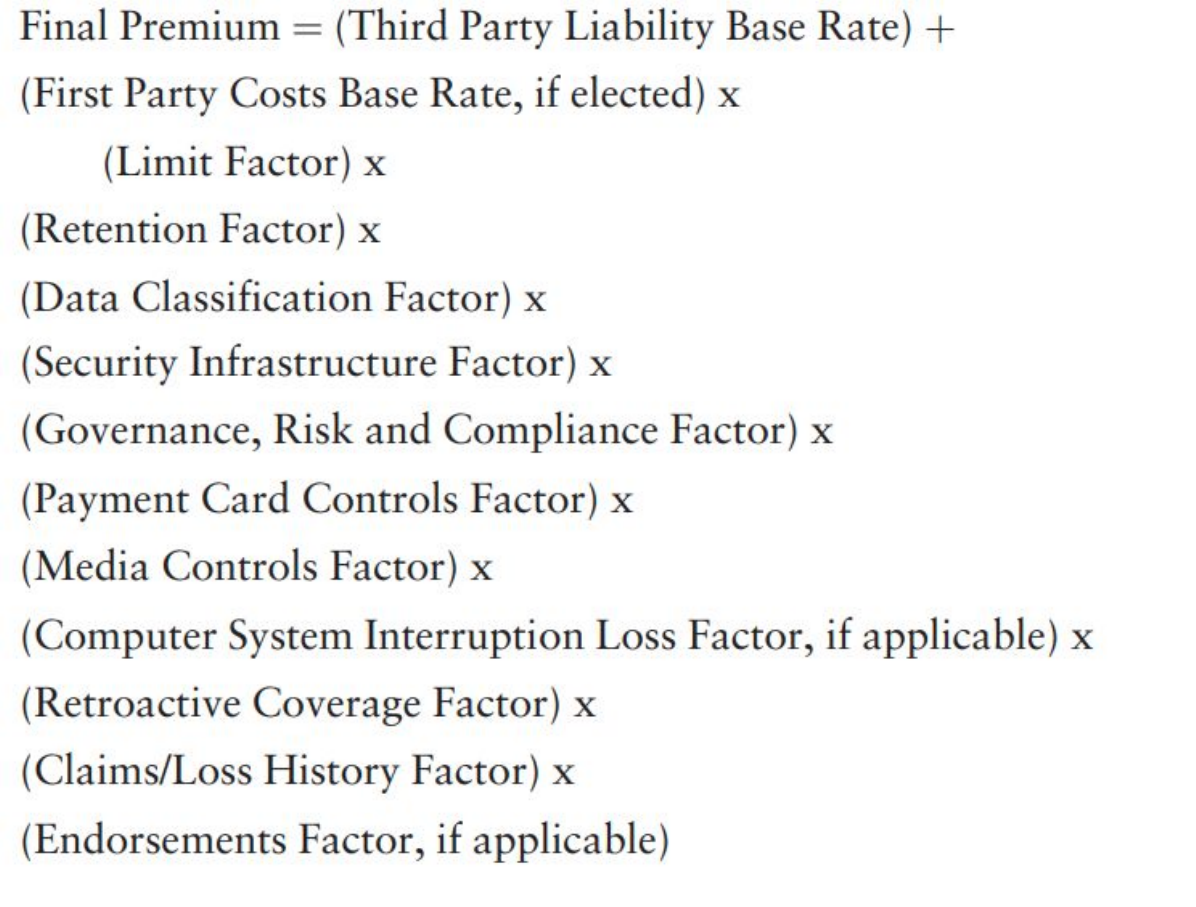
Table 14: Security factor weighting[a]

Rating	Weighting
Excellent	0.75–0.85
Good	0.85–1.00
Fair	1.00–1.25
Poor	1.25–1.50

[a] *Source*: POL-64. See also POL-41.



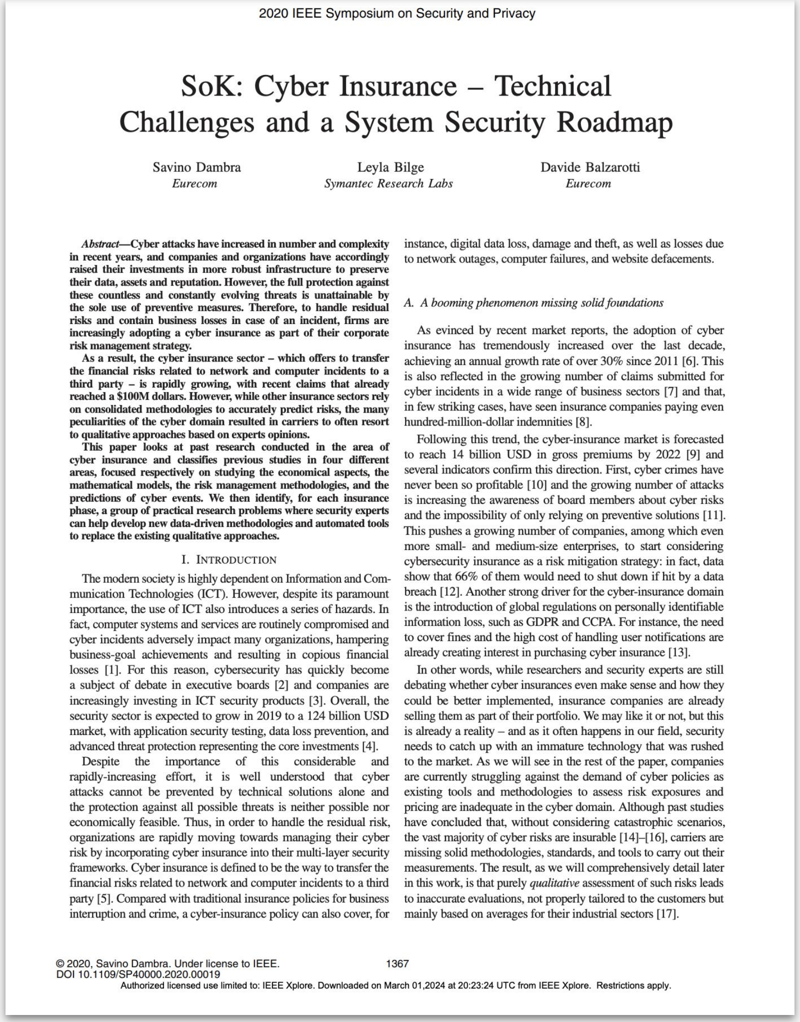
Premium = [Base Premium] x
[Loss Rating] x
[Professional Experience] x
[Longevity of Operations] x
[Use of Written Contracts] x
[Risk Characteristics] x
[Prior Acts Factor] x
[Coverage Adjustment] x
[Deductible]



Final Premium = (Third Party Liability Base Rate) +
(First Party Costs Base Rate, if elected) x
(Limit Factor) x
(Retention Factor) x
(Data Classification Factor) x
(Security Infrastructure Factor) x
(Governance, Risk and Compliance Factor) x
(Payment Card Controls Factor) x
(Media Controls Factor) x
(Computer System Interruption Loss Factor, if applicable) x
(Retroactive Coverage Factor) x
(Claims/Loss History Factor) x
(Endorsements Factor, if applicable)

Napkin math

- Likelihood of ransomware incident: 23%
- Average cost of ransomware event: $2M
- Expected loss : $460K
- Average premium



2020 IEEE Symposium on Security and Privacy

SoK: Cyber Insurance – Technical Challenges and a System Security Roadmap

Savino Dambra
Eurecom

Leyla Bilge
Symantec Research Labs

Davide Balzarotti
Eurecom

***Abstract*—Cyber attacks have increased in number and complexity in recent years, and companies and organizations have accordingly raised their investments in more robust infrastructure to preserve their data, assets and reputation. However, the full protection against these countless and constantly evolving threats is unattainable by the sole use of preventive measures. Therefore, to handle residual risks and contain business losses in case of an incident, firms are increasingly adopting a cyber insurance as part of their corporate risk management strategy.**

As a result, the cyber insurance sector – which offers to transfer the financial risks related to network and computer incidents to a third party – is rapidly growing, with recent claims that already reached a $100M dollars. However, while other insurance sectors rely on consolidated methodologies to accurately predict risks, the many peculiarities of the cyber domain resulted in carriers to often resort to qualitative approaches based on experts opinions.

This paper looks at past research conducted in the area of cyber insurance and classifies previous studies in four different areas, focused respectively on studying the economical aspects, the mathematical models, the risk management methodologies, and the predictions of cyber events. We then identify, for each insurance phase, a group of practical research problems where security experts can help develop new data-driven methodologies and automated tools to replace the existing qualitative approaches.

I. Introduction

The modern society is highly dependent on Information and Communication Technologies (ICT). However, despite its paramount importance, the use of ICT also introduces a series of hazards. In fact, computer systems and services are routinely compromised and cyber incidents adversely impact many organizations, hampering business-goal achievements and resulting in copious financial losses [1]. For this reason, cybersecurity has quickly become a subject of debate in executive boards [2] and companies are increasingly investing in ICT security products [3]. Overall, the security sector is expected to grow in 2019 to a 124 billion USD market, with application security testing, data loss prevention, and advanced threat protection representing the core investments [4].

Despite the importance of this considerable and rapidly-increasing effort, it is well understood that cyber attacks cannot be prevented by technical solutions alone and the protection against all possible threats is neither possible nor economically feasible. Thus, in order to handle the residual risk, organizations are rapidly moving towards managing their cyber risk by incorporating cyber insurance into their multi-layer security frameworks. Cyber insurance is defined to be the way to transfer the financial risks related to network and computer incidents to a third party [5]. Compared with traditional insurance policies for business interruption and crime, a cyber-insurance policy can also cover, for instance, digital data loss, damage and theft, as well as losses due to network outages, computer failures, and website defacements.

A. *A booming phenomenon missing solid foundations*

As evinced by recent market reports, the adoption of cyber insurance has tremendously increased over the last decade, achieving an annual growth rate of over 30% since 2011 [6]. This is also reflected in the growing number of claims submitted for cyber incidents in a wide range of business sectors [7] and that, in few striking cases, have seen insurance companies paying even hundred-million-dollar indemnities [8].

Following this trend, the cyber-insurance market is forecasted to reach 14 billion USD in gross premiums by 2022 [9] and several indicators confirm this direction. First, cyber crimes have never been so profitable [10] and the growing number of attacks is increasing the awareness of board members about cyber risks and the impossibility of only relying on preventive solutions [11]. This pushes a growing number of companies, among which even more small- and medium-size enterprises, to start considering cybersecurity insurance as a risk mitigation strategy: in fact, data show that 66% of them would need to shut down if hit by a data breach [12]. Another strong driver for the cyber-insurance domain is the introduction of global regulations on personally identifiable information loss, such as GDPR and CCPA. For instance, the need to cover fines and the high cost of handling user notifications are already creating interest in purchasing cyber insurance [13].

In other words, while researchers and security experts are still debating whether cyber insurances even make sense and how they could be better implemented, insurance companies are already selling them as part of their portfolio. We may like it or not, but this is already a reality – and as it often happens in our field, security needs to catch up with an immature technology that was rushed to the market. As we will see in the rest of the paper, companies are currently struggling against the demand of cyber policies as existing tools and methodologies to assess risk exposures and pricing are inadequate in the cyber domain. Although past studies have concluded that, without considering catastrophic scenarios, the vast majority of cyber risks are insurable [14]–[16], carriers are missing solid methodologies, standards, and tools to carry out their measurements. The result, as we will comprehensively detail later in this work, is that purely *qualitative* assessment of such risks leads to inaccurate evaluations, not properly tailored to the customers but mainly based on averages for their industrial sectors [17].

DOI 10.1109/SP40000.2020.00019

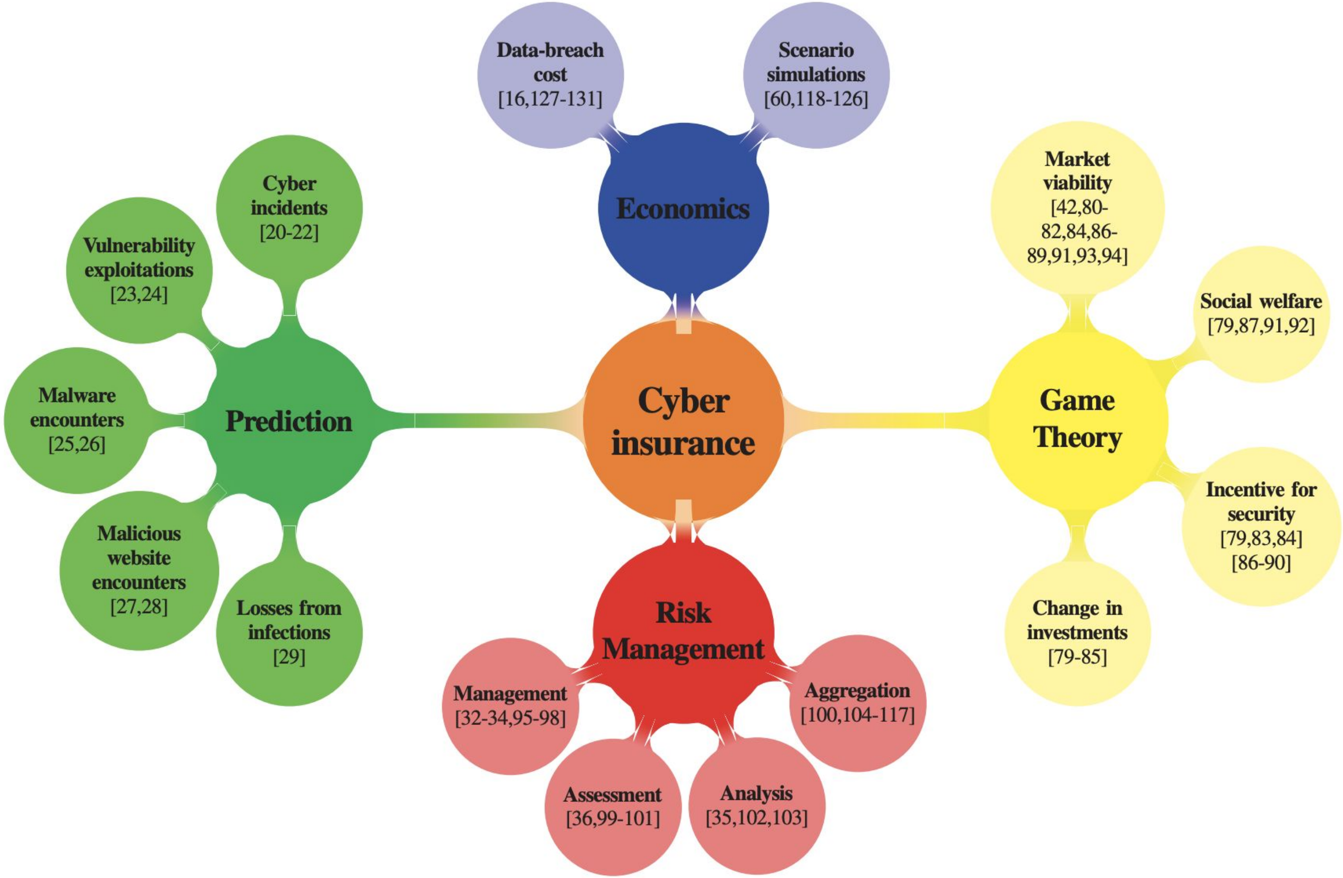

Economics
Data-breach cost [16,127-131]
Scenario simulations [60,118-126]
Prediction
Cyber incidents [20-22]
Vulnerability exploitations [23,24]
Malware encounters [25,26]
Malicious website encounters [27,28]
Losses from infections [29]
Cyber insurance
Game Theory
Market viability [42,80-82,84,86-89,91,93,94]
Social welfare [79,87,91,92]
Incentive for security [79,83,84] [86-90]
Change in investments [79-85]
Risk Management
Management [32-34,95-98]
Assessment [36,99-101]
Analysis [35,102,103]
Aggregation [100,104-117]

Fig. 2: Cyber-insurance research areas

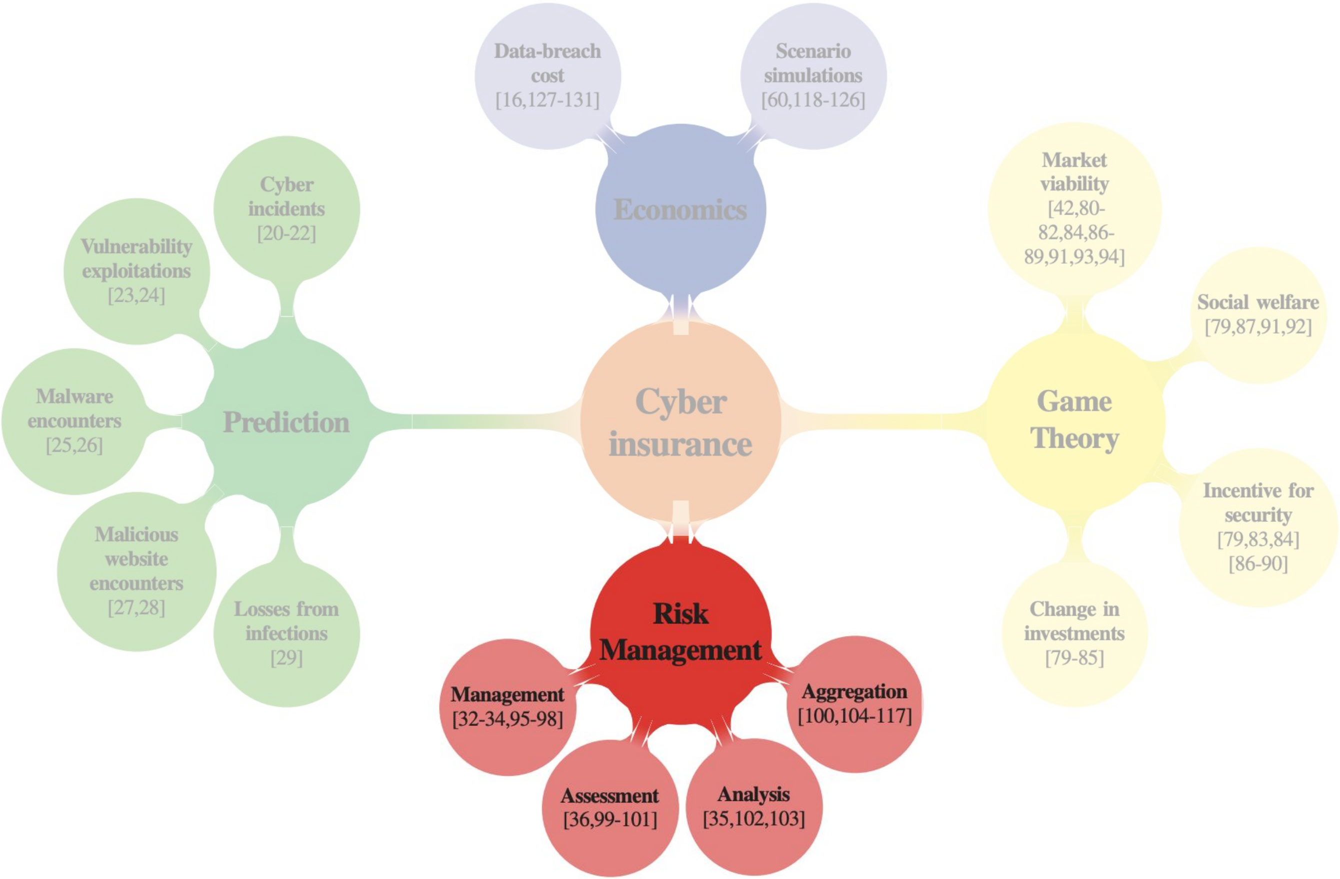

Data-breach cost [16,127-131]
Scenario simulations [60,118-126]
Economics
Cyber incidents [20-22]
Vulnerability exploitations [23,24]
Malware encounters [25,26]
Prediction
Malicious website encounters [27,28]
Losses from infections [29]
Cyber insurance
Market viability [42,80-82,84,86-89,91,93,94]
Social welfare [79,87,91,92]
Game Theory
Incentive for security [79,83,84] [86-90]
Change in investments [79-85]
Risk Management
Management [32-34,95-98]
Aggregation [100,104-117]
Assessment [36,99-101]
Analysis [35,102,103]

Fig. 2: Cyber-insurance research areas

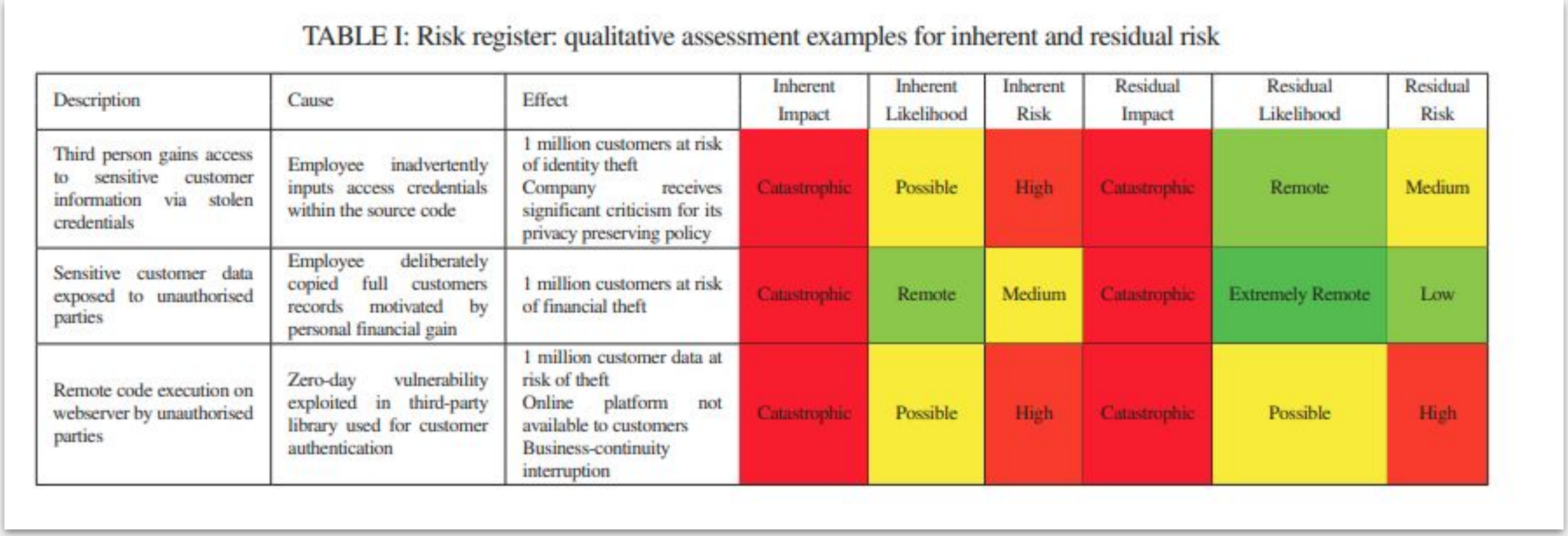


TABLE I: Risk register: qualitative assessment examples for inherent and residual risk

Description	Cause	Effect	Inherent Impact	Inherent Likelihood	Inherent Risk	Residual Impact	Residual Likelihood	Residual Risk
Third person gains access to sensitive customer information via stolen credentials	Employee inadvertently inputs access credentials within the source code	1 million customers at risk of identity theft Company receives significant criticism for its privacy preserving policy	Catastrophic	Possible	High	Catastrophic	Remote	Medium
Sensitive customer data exposed to unauthorised parties	Employee deliberately copied full customers records motivated by personal financial gain	1 million customers at risk of financial theft	Catastrophic	Remote	Medium	Catastrophic	Extremely Remote	Low
Remote code execution on webserver by unauthorised parties	Zero-day vulnerability exploited in third-party library used for customer authentication	1 million customer data at risk of theft Online platform not available to customers Business-continuity interruption	Catastrophic	Possible	High	Catastrophic	Possible	High

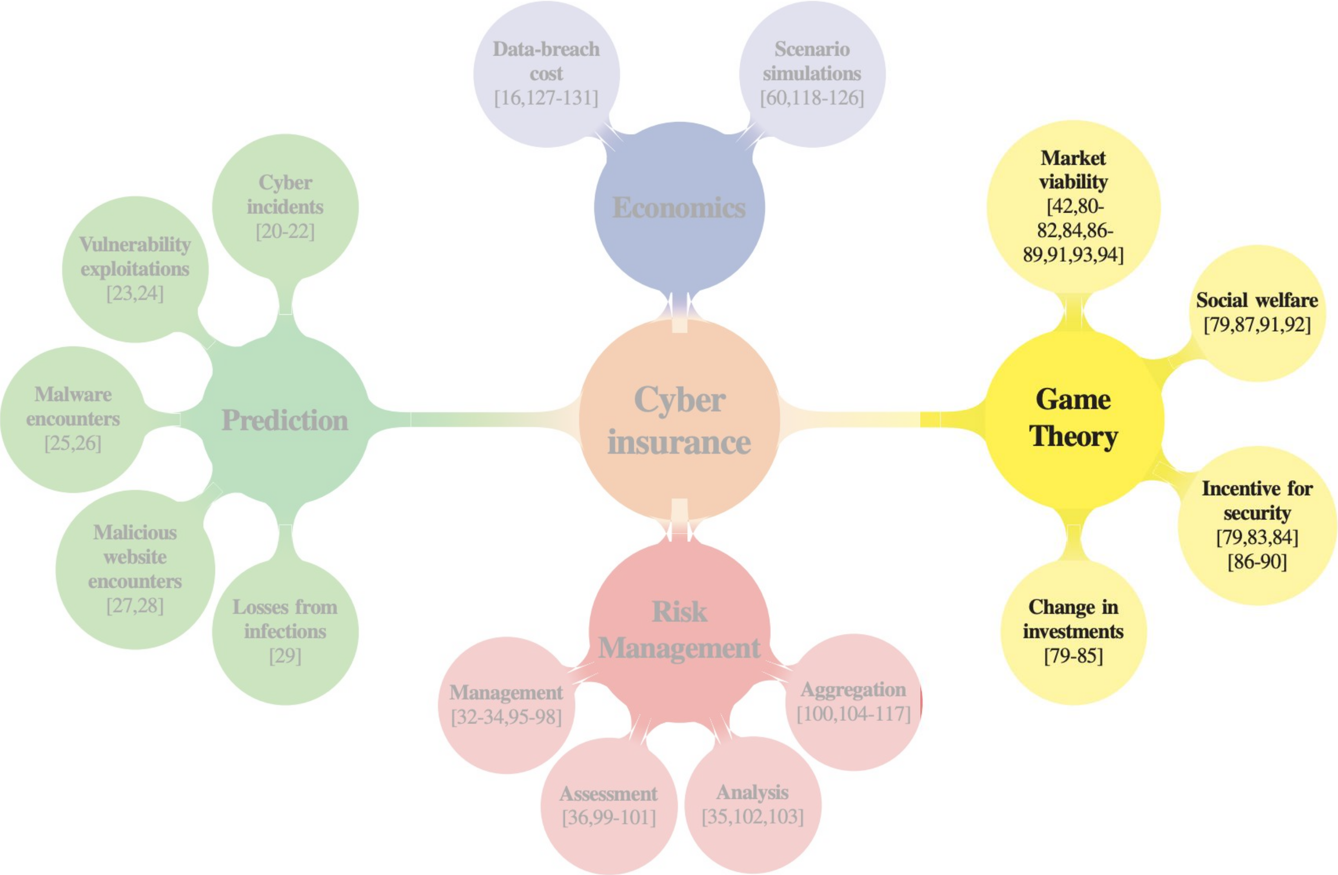

Cyber insurance
Economics
Data-breach cost [16,127-131]
Scenario simulations [60,118-126]
Game Theory
Market viability [42,80-82,84,86-89,91,93,94]
Social welfare [79,87,91,92]
Incentive for security [79,83,84] [86-90]
Change in investments [79-85]
Risk Management
Management [32-34,95-98]
Assessment [36,99-101]
Analysis [35,102,103]
Aggregation [100,104-117]
Prediction
Cyber incidents [20-22]
Vulnerability exploitations [23,24]
Malware encounters [25,26]
Malicious website encounters [27,28]
Losses from infections [29]

Fig. 2: Cyber-insurance research areas

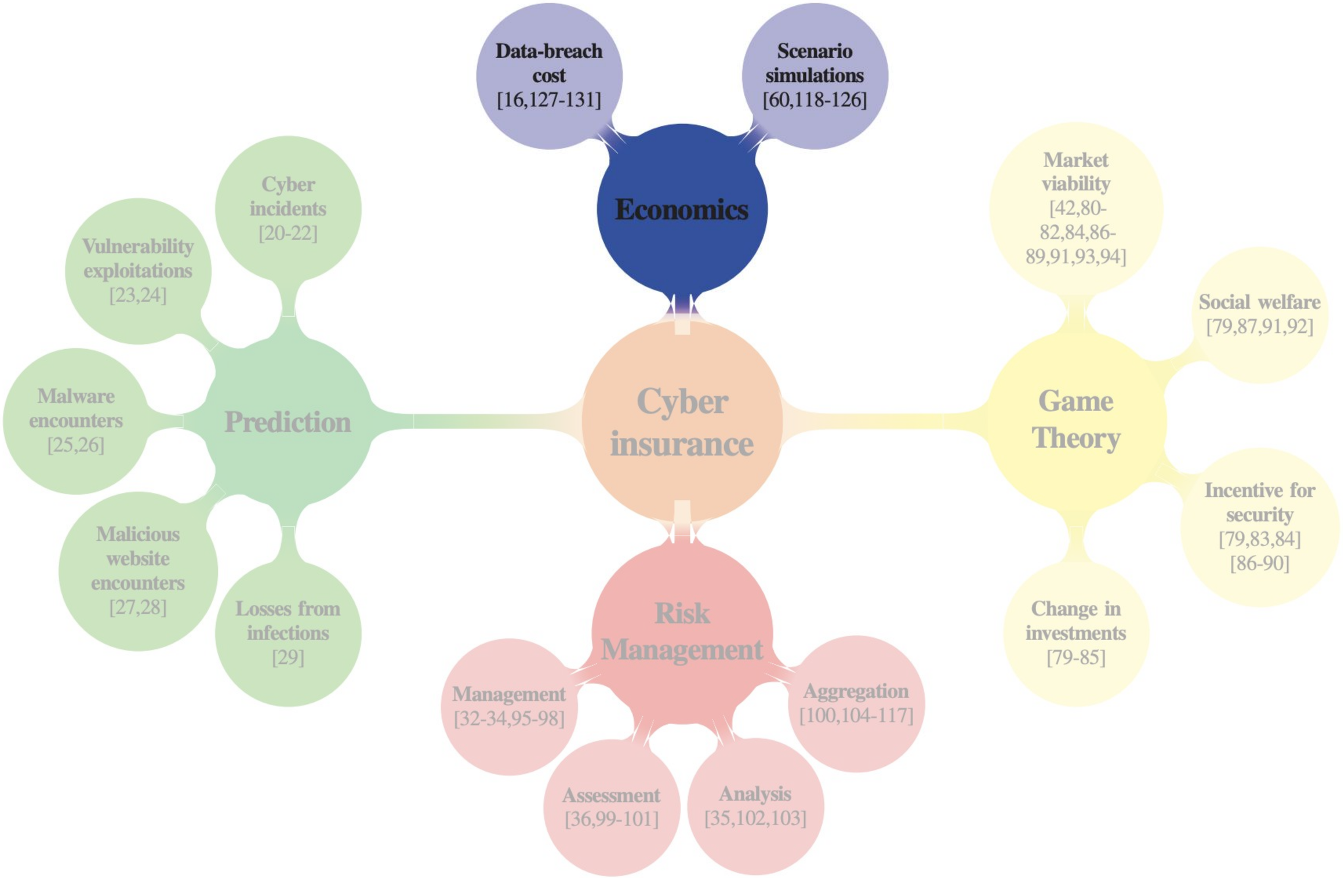

Data-breach cost [16,127-131]
Scenario simulations [60,118-126]
Economics
Market viability [42,80-82,84,86-89,91,93,94]
Social welfare [79,87,91,92]
Game Theory
Incentive for security [79,83,84] [86-90]
Change in investments [79-85]
Cyber incidents [20-22]
Vulnerability exploitations [23,24]
Malware encounters [25,26]
Prediction
Cyber insurance
Malicious website encounters [27,28]
Losses from infections [29]
Risk Management
Management [32-34,95-98]
Aggregation [100,104-117]
Assessment [36,99-101]
Analysis [35,102,103]

Fig. 2: Cyber-insurance research areas

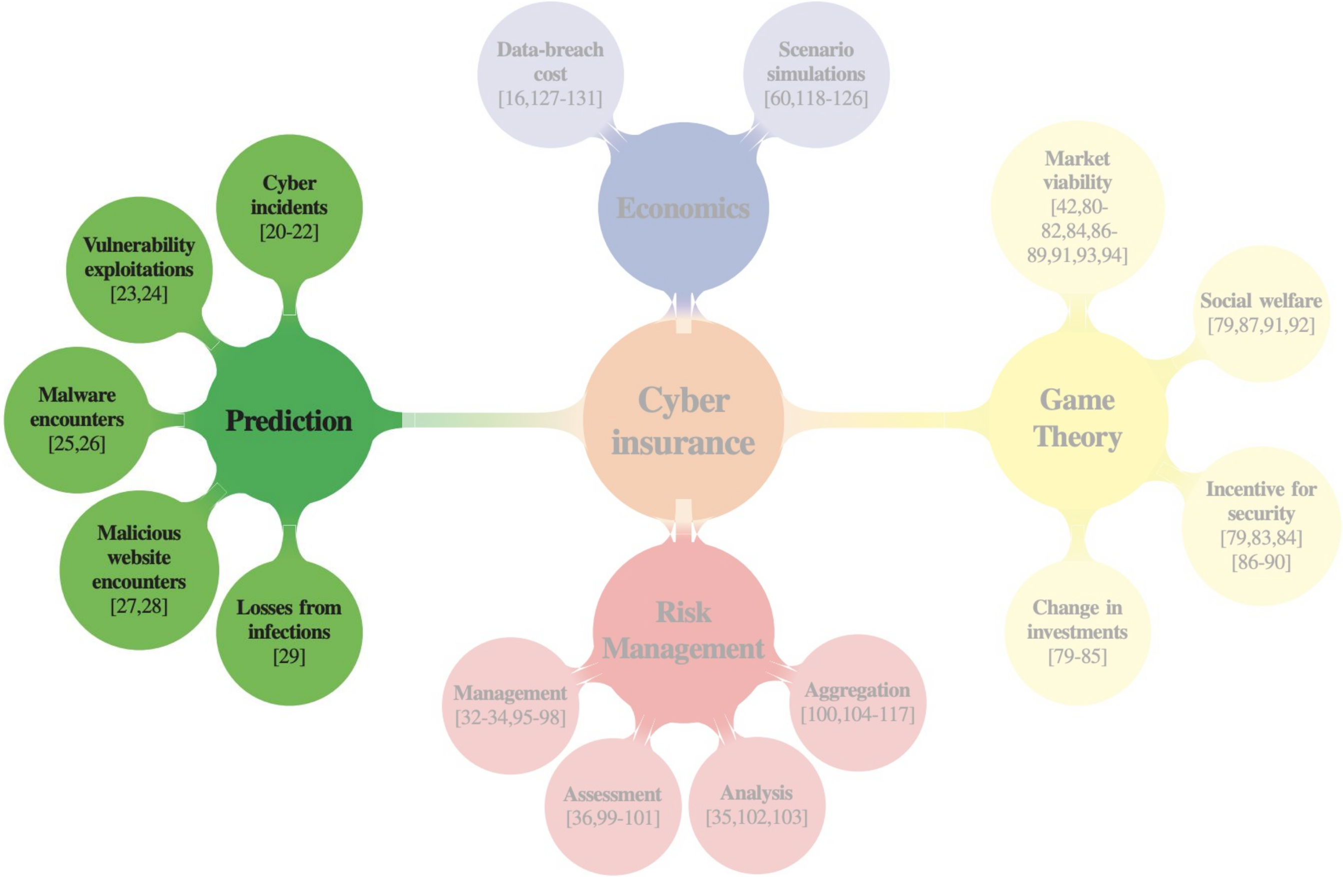

Data-breach cost [16,127-131]
Scenario simulations [60,118-126]
Economics
Cyber incidents [20-22]
Vulnerability exploitations [23,24]
Malware encounters [25,26]
Prediction
Malicious website encounters [27,28]
Losses from infections [29]
Cyber insurance
Market viability [42,80-82,84,86-89,91,93,94]
Social welfare [79,87,91,92]
Game Theory
Incentive for security [79,83,84] [86-90]
Change in investments [79-85]
Risk Management
Management [32-34,95-98]
Aggregation [100,104-117]
Assessment [36,99-101]
Analysis [35,102,103]

Fig. 2: Cyber-insurance research areas

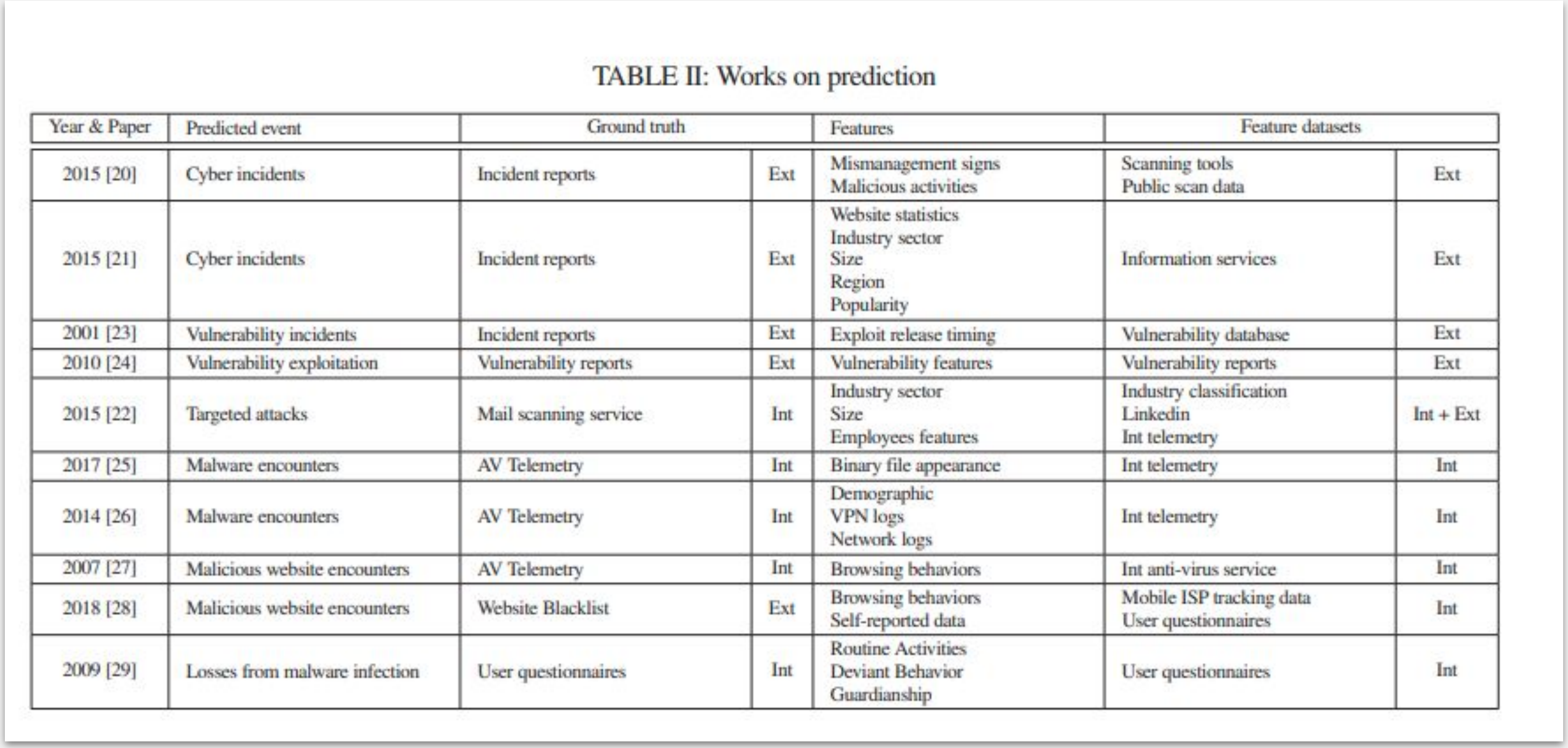


TABLE II: Works on prediction

Year & Paper	Predicted event	Ground truth		Features	Feature datasets	
2015 [20]	Cyber incidents	Incident reports	Ext	Mismanagement signs Malicious activities	Scanning tools Public scan data	Ext
2015 [21]	Cyber incidents	Incident reports	Ext	Website statistics Industry sector Size Region Popularity	Information services	Ext
2001 [23]	Vulnerability incidents	Incident reports	Ext	Exploit release timing	Vulnerability database	Ext
2010 [24]	Vulnerability exploitation	Vulnerability reports	Ext	Vulnerability features	Vulnerability reports	Ext
2015 [22]	Targeted attacks	Mail scanning service	Int	Industry sector Size Employees features	Industry classification Linkedin Int telemetry	Int + Ext
2017 [25]	Malware encounters	AV Telemetry	Int	Binary file appearance	Int telemetry	Int
2014 [26]	Malware encounters	AV Telemetry	Int	Demographic VPN logs Network logs	Int telemetry	Int
2007 [27]	Malicious website encounters	AV Telemetry	Int	Browsing behaviors	Int anti-virus service	Int
2018 [28]	Malicious website encounters	Website Blacklist	Ext	Browsing behaviors Self-reported data	Mobile ISP tracking data User questionnaires	Int
2009 [29]	Losses from malware infection	User questionnaires	Int	Routine Activities Deviant Behavior Guardianship	User questionnaires	Int

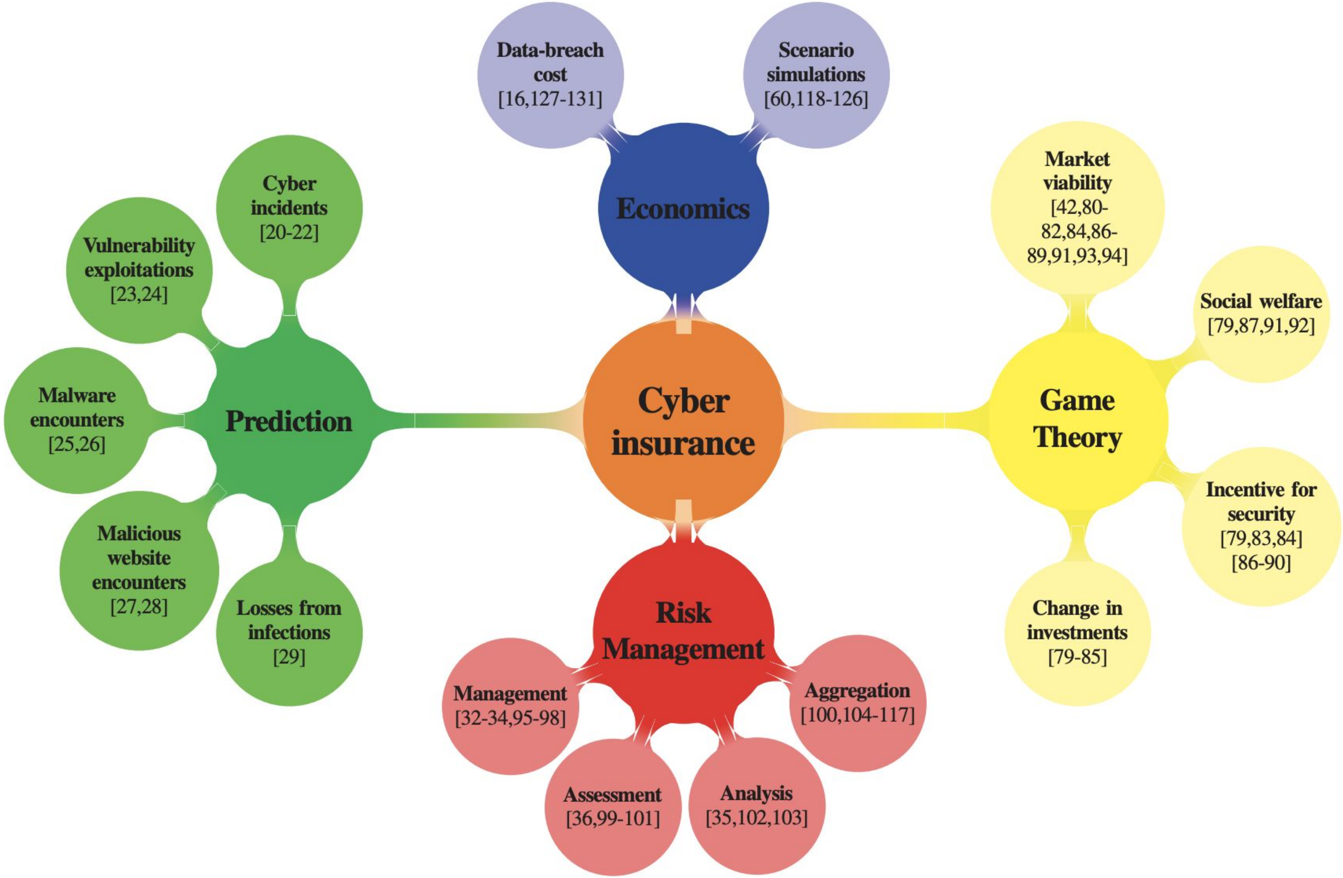

Data-breach cost [16,127-131]
Scenario simulations [60,118-126]
Economics
Cyber incidents [20-22]
Vulnerability exploitations [23,24]
Malware encounters [25,26]
Prediction
Malicious website encounters [27,28]
Losses from infections [29]
Cyber insurance
Market viability [42,80-82,84,86-89,91,93,94]
Social welfare [79,87,91,92]
Game Theory
Incentive for security [79,83,84] [86-90]
Change in investments [79-85]
Risk Management
Management [32-34,95-98]
Aggregation [100,104-117]
Assessment [36,99-101]
Analysis [35,102,103]

Fig. 2: Cyber-insurance research areas

Why should the systems security community care about insurance?

1. “Help the development of quantitative, data-driven methodologies”
2. “Bring automation and support tools to replace questionnaires and qualitative estimations”

Area #1: Risk Prediction

- Measure the security posture of the target
- Measure the behavior of the target
- Measure the attack surface
- Influence of business sector, reputation, and assets of an organization
- Predict future events based on historical data
- Measure the risk that propagates through third-party relations
- Users’ weakness and social engineering
- Risk aggregation

Area #2: Automated Data Collection

- Romanosky et al. show that security questionnaires are very superficial
- “Nevertheless, the extent to which security standards compliance reflect the level of risk a company faces has not been yet understood **<R12>**”

Area #3: Catastrophe modeling

- Build service dependency graphs
  - Update since 2020: Current regulatory push for SBOMs
  - Hindered by dynamic nature of dependencies, hidden backups, etc.

Area #4: Forensic analysis

- How to prevent the cyber equivalent of burning down your house for the insurance money
    - Is this a task for researchers or for practitioners?

Cyber Insurance

COMS6998 sec:12
Economics of Cybersecurity
5 March 2024

“An insurance salesman in an office, selling a cyber insurance policy to a concerned business executive”