The Harel Center for Capital Markets Research
Coller School of Management
Tel Aviv university

Global Cyber Insurance – A Meta-Analysis

April 2023

Dan Weiss and Naomi Shpirer Belfer

What is Meta-analysis?

Meta-analysis is a research process used to systematically integrate the data and findings from independent studies, using statistical methods to calculate an overall effect.

All the presented figures are Harel Center estimations and analyses based on publically available data and figures in prior studies.
We thank Bar Sobel for outstanding research assistance.

List of Studies

A Research Agenda for Cyber Risk and Cyber Insurance, : Gregory Falco et al., The Center for International Security and Cooperation, Stanford University, 2020.

An Empirical Analysis of Insurer Participation in the U.S. Cyber Insurance Market, Cassandra R. Cole & Stephen G. Fier, North American Actuarial Journal, 2021.

The Role of Insurance in Cyber Risk Management in Enterprises, Bartłomiej Balawejder et al., Humanities and Social Sciences, 2019.

Cyber Loss Distribution Fitting: A General Framework towards Cyber Bonds and Their Pricing Models, Oleg Kolesnikov et al., International Journal of Mathematics and Mathematical Sciences, 2022.

Insurability of Cyber Risk: An Empirical Analysis, Christian Biener et al., The Geneva Papers, 2015.

Cyber Risk Management in the US Banking and Insurance Industry: A Textual and Empirical Analysis of Determinants and Value, Nadine Gatzert and Madeline Schubert, Journal of Risk and Insurance, 2022.

Cyber Insurance and Private Governance: The Enforcement Power of Markets, Trey Herr, Regulation & Governance, 2021.

Cyber Insurance Offering and Performance: An Analysis of the U.S. Cyber Insurance Market, Xiaoying Xie et al., The Geneva Papers on Risk and Insurance - Issues and Practice , 2020.

Insurance and Enterprise: Cyber Insurance for Ransomware, Tom Baker and Anja Shortland, The Geneva Papers on Risk and Insurance - Issues and Practice , 2022.

Content Analysis of Cyber Insurance Policies: How Do Carriers Price Cyber Risk? Sasha Romanosky, Journal of Cybersecurity, 2019.

Understanding Systemic Cyber Risk, World Economic Forum, 2016.

As Cyber Insurance Dries Up, Treasury Department Eyes a Backstop, Bloomberg Law, Oct 2022.

Report on the Effectiveness of the Terrorism Risk Insurance Program, Federal Insurance Office, U.S. Department of the Treasury, Jun 2022.

Challenges in Securing Federal Systems and Information, GAO US Government Accountability Office, 2023.

Memorandum, NAIC, Oct 2022.

Insuring Hostile Cyber Activity: In Search of Sustainable Solutions , Rachel Anne Carter et al., The Geneva Association, 2022.

How Has Ransomware Changed Cyber Insurance? Pedro Ernesto Aquino, California State University, 2022.

War, Terrorism, and Catastrophe in Cyber Insurance: Understanding and Reforming Exclusions ,Jon Bateman, Carnegie Endowment for International Peace, 2020.

Action Needed to Assess Potential Federal Response to Catastrophic Attacks, GAO United States Government Accountability Office, Jun 2022.

Potential Federal Insurance Response to Catastrophic Cyber Incidents, The U.S. Department of the Treasury, 2022.

Understanding Cyber Insurance - A Structured Dialogue with Insurance Companies, EIOPA, 2018.

Setting the Scene: Framing Catastrophic Cyber Risk, Unal Tatar et al., SOA Research Institute, 2023.

Financial Statements 2022 – Aegon, Allianz, Aviva, AXA, Chubb, Fairfax, , Generali ,NN Group, RSA.

Cyber Insurance Policies - Allianz, Aviva, Chubb, RSA, איילון, הפניקס, הראל הבשרה, כלל

Commercial Reports – Coveware 2023, Marsh 2022, AON 2022, 2023, Gallagher Re 2020, 2021, McAfee 2020, Willis Towers Watson 2020, Munich Re 2021, Kovrr 2020, Guy Carpenter and CyberCube 2019, McKinsey 2022, EY 2022, KPMG 2022, Delloite 2022, PWC 2021.

Quarterly Cyber Insurance Update, Wall Street Journal :Feb 2023.

Cyber Attacks Set to Become ‘Uninsurable’,sSys Zurich Chief, Financial Times, Ian Smith, Feb 2023.

SolarWinds Agrees to $26 Million Payout Over Massive Data Breach, Insights ISS Governance, Nov 2022.

Cost of a Data Breach Report, IBM, 2022

מהו סייבר? חלק ב: אתגרי האסדרה של הגנת הסייבר, רחל אריזור הרשקוביץ תהילה שוורץ אלטשולר , המכון הישראלי לדמוקרטיה, 2023.

ניהול סיכוני סייבר בגופים מוסדיים, משרד האוצר אגף שוק ההון, ביטוח וחסכון, 2016.

ניהול סיכוני סייבר בנותני שירותים פיננסיים, רשות שוק ההון, 2022.

דוח ריכוז ממצאי ביקורת רוחב בנושא סיכוני סייבר בתאגיד מדווח, רשות ניירות ערך, ינואר 2023

Agenda

1. Objectives
2. Early stage issues in cyber insurance
3. Cyber insurance – A snapshot
    - 3.1 Premiums and underwriting
    - 3.2 Claims and profitability
    - 3.3 Reinsurance
4. Regulatory status
5. Summary – What do we take-away?

Objectives

1. Identify the current market and regulatory status.
2. Outline future development of the cyber insurance market (and business opportunities for insurers).

Cyber Insurance

"Cyber insurance is an increasingly significant risk-transfer mechanism, and the insurance industry has an important role to play in strengthening cyber hygiene and building resiliency, including combatting ransomware."

Annual Report on the Insurance Industry, Federal Insurance Office, U.S. Department of the Treasury, September 2022, page 7.

Early Stage Issues in Cyber Insurance

- Does a P&C policy cover **silent cyber exposures**? For example, are loss of profits or a fire in a facility caused by shutting down a programmable controller covered by standard P&C policies? LLOYDS
- Coverage offered by **affirmative cyber policies**
  - First party: event management/breach response, loss from business/network interruption, cyber extortion/ransomware, data restoration.
  - Third party: privacy liability, network security liability, privacy regulatory defense costs.
- Underwriting difficulties - catastrophic cyber perils do not have well-established definitions or fundamental physical properties. For these reasons, catastrophic cyber events have the inherent potential for significant economic loss. Lack of data and competence prohibits a link between premium and exposure.
- Loss prevention? – young technologies, weak proficiency.
- **Systemic attacks and war, terror, etc. – Is cyber risk insurable?**

War Exclusion (2022 version)

War

arising from any physical act of war, invasion, or warlike operations (whether war be declared or not), civil war, riot, civil commotion, rebellion, revolution, insurrection, civil uprising or military or usurped power.

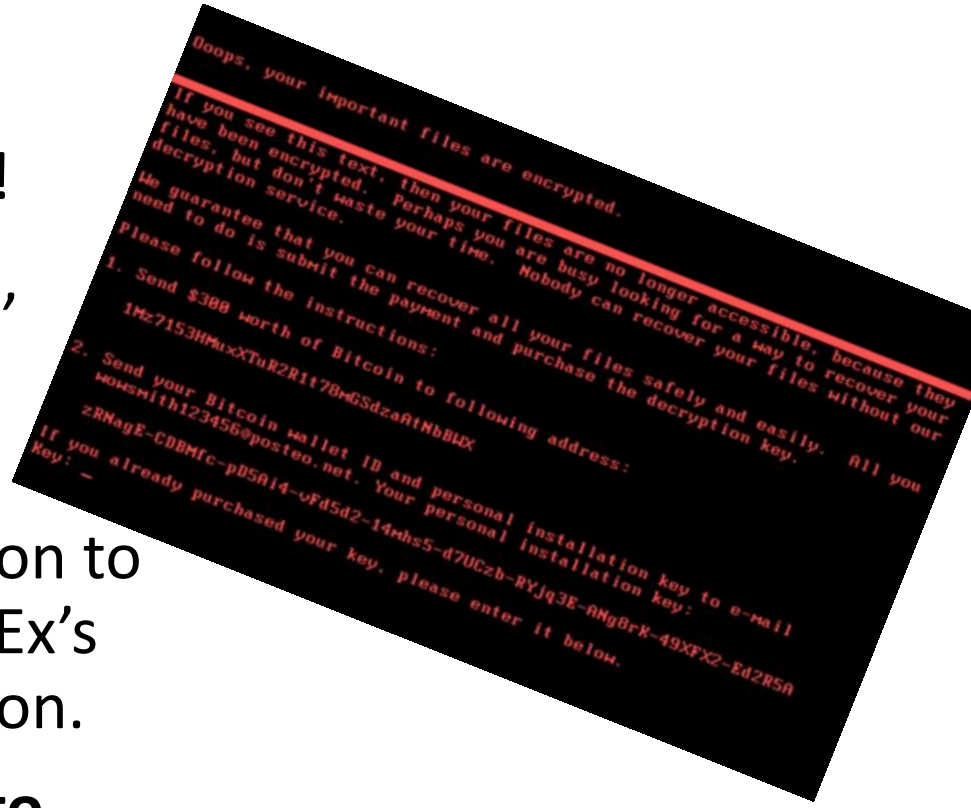
מלחמה

פוליסה זו אינה מכסה אובדן, נזק, הפסד או חבות מכל סוג, הנובעים או הקשורים במישרין או בעקיפין ל:

מלחמה, פלישה, פעולת אויב זר, פעולות איבה, מלחמת אזרחים, מרד, הפיכה, התקוממות, כוח צבאי, תפיסת שלטון בכוח, הלאמה, החרמה או הרס של **מערכות המחשב של המבוטח** או של **מסד נתונים** בפקודת רשות ציבורית או ממשלתית.

כל פעולת טרור; השבתה ופעולת עבודה דומה, מלחמה, פלישה, פעולת אויב זר, פעולות איבה או פעולות מלחמתיות (בין אם הוכרזו ובין אם לאו), מלחמת אזרחים, מרד, מהומות אזרחיות בעלות מימדים של או בהיקף של התקוממות עממית, התקוממות צבאית, התקוממות, מרד, מהפכה, תפיסת שלטון צבאית או בידי כוח אחר, או כל פעולה שננקטה כדי לעכב או להגן מפני פעולות אלה; כולל כל הסכומים, נזקים, או הוצאות משפט מכל סוג שהוא, במישרין או בעקיפין שנגרמו או הנובעים או בקשר עם כל פעולה שננקטה לשם שליטה, מניעה, דיכוי, או הקשורים בכל דרך שהיא לאמור לעיל; עם זאת, אם אנו טוענים כי בשל החרגה זו כל נזק או הוצאות משפט אינם מכוסים על ידי מדיניות זו, נטל הוכחת ההיפך יהיה על המבוטח. יחד עם זאת, החרגה זה אינה חלה על פעולות שבוצעו באופן אלקטרוני.

NotPetya – Exclusion of War Actions

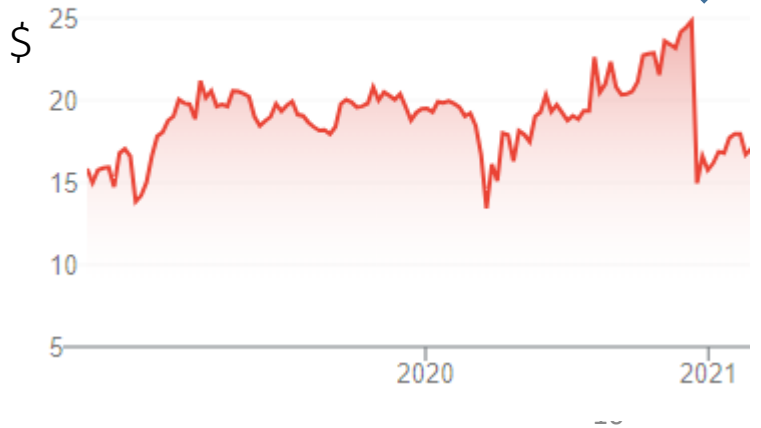


- The most destructive malware ever (June 2017)!
- Ukraine was the target of a Russia-backed effort, spread across Europe, the UK and farther.
- Not a ransomware attack.
- Damages: $870 million loss to Merck, $100 million to Mondelez (Oreos, Ritz), and $400 million to FedEx's European subsidiary. Total estimated at $10 billion.
- **Zurich refused to cover the $100 million claim to Mondelez due to exclusion of "act of war".**
- **Settlement (Oct 2022).**

SolarWinds (NYSE SWI) - 2020

- SolarWinds was subject to a massive data breach by hackers who injected malicious code into the company's "Orion" software (Dec 2020).
- Investors filed a securities class action, alleging that SolarWinds falsely and misleadingly told investors that it had a robust cybersecurity program and adhered the cybersecurity practices in the "Security Statement" on its website.
- A $26 million tentative settlement (Nov 2022).

SWI stock price dropped 40%!



Systemic Cyber Risk

- Systemic cyber risk is the risk that a cyber event at an individual component of a critical infrastructure ecosystem will cause significant harm not only in the originating component but consequences also cascade into the ecosystem.
- Systemic cyber risk quantification models that consider and include the tail risk of multiple cascading consequences are needed.
- Particularly, the threat expands to significant adverse effects to public health or safety, economic security or national security, beyond claims from the private insurance industry.
- Understanding how the government will respond during a national cyber incident will enable the private sector to tailor its expectations and to plug into the larger effort as appropriate.

Premiums

- The property-casualty insurance industry has gone through a meaningful growth in the cyber insurance market over the past five years, largely attributable to the expansion of digital technology coupled with the increasing frequency of cyber attacks.
- Demand for cyber insurance by corporations is continuing to soar and premium rates have substantially increased in 2021-2022.
- Analysts expect the cyber insurance market to continue growing, doubling in the next three years.
- Trend: a cyber insurance policy includes both monetary coverage and a professional response team.
- The #1 sales trigger - 40% of companies in the US purchased cybersecurity insurance when a cyberattack occurred on another organization in the same industry.

3. Cyber insurance – A snapshot

Chart 1

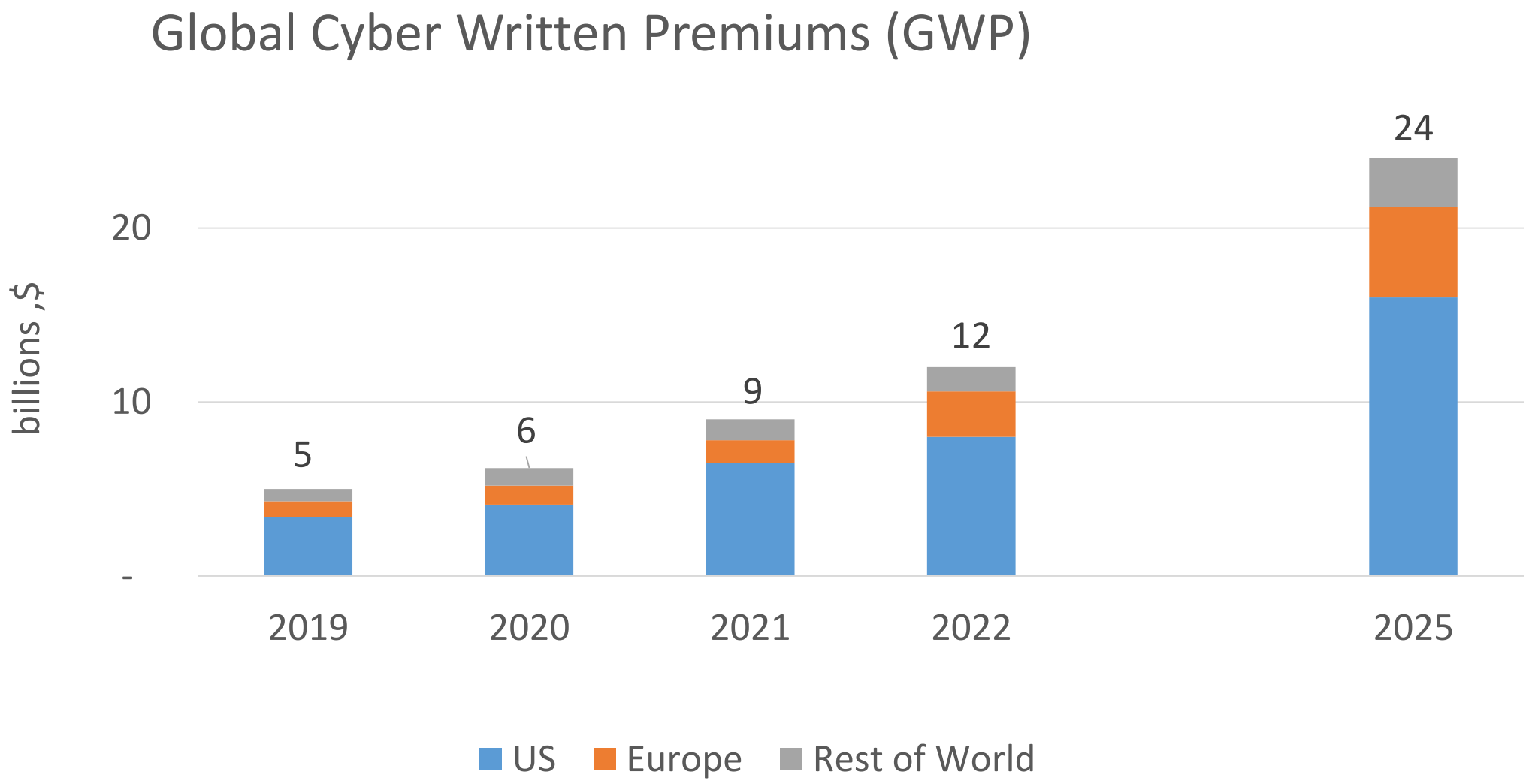


Chart 2

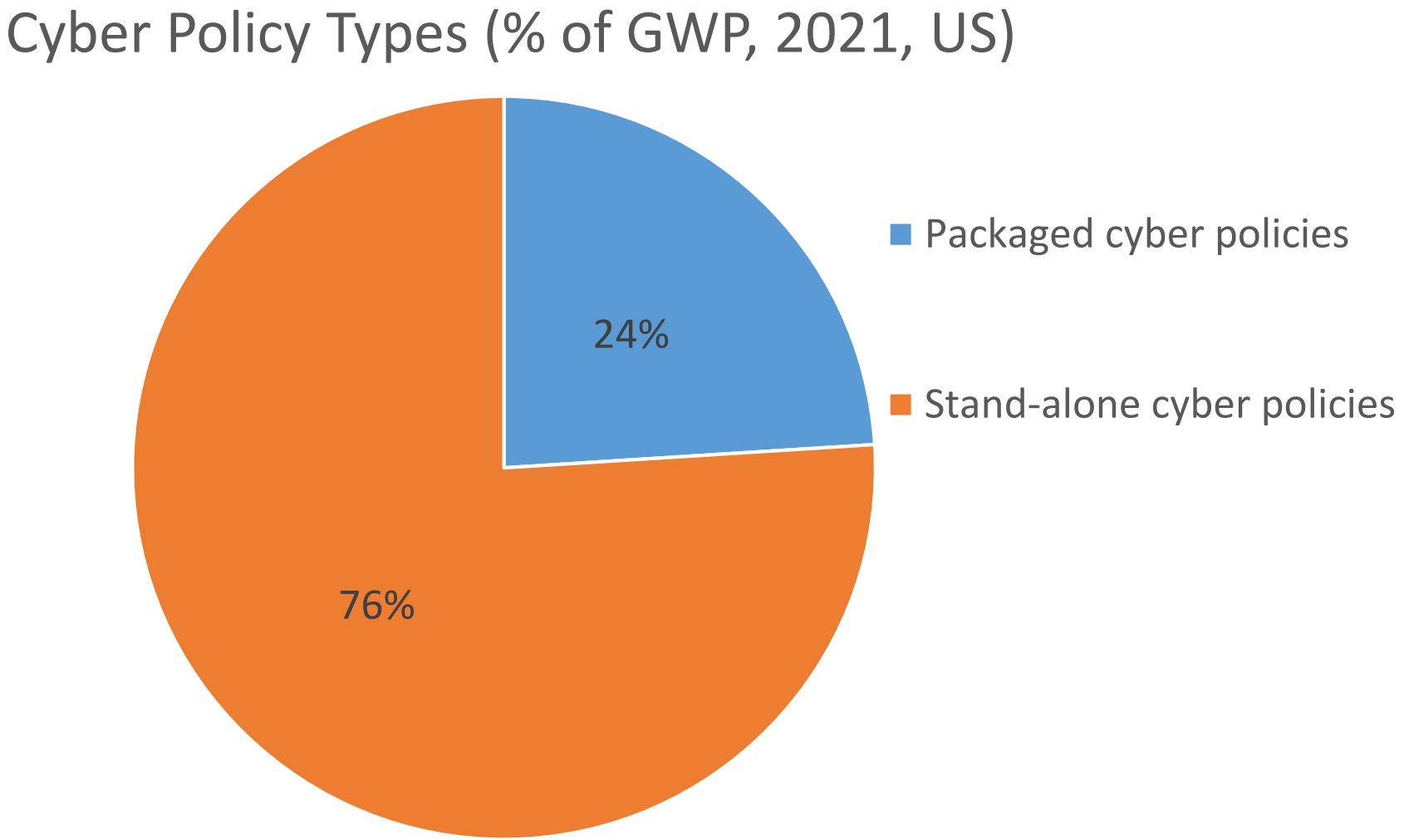
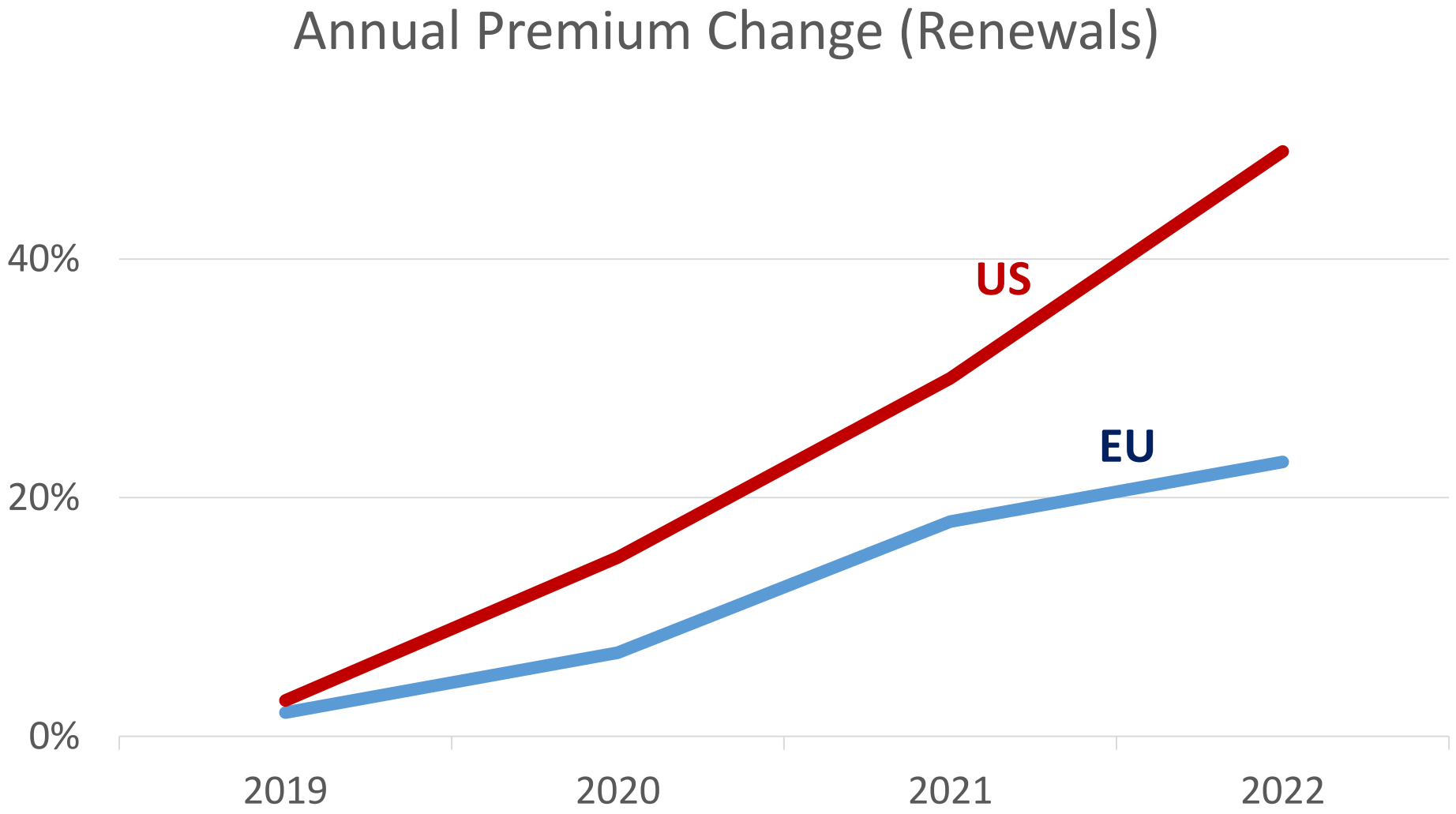
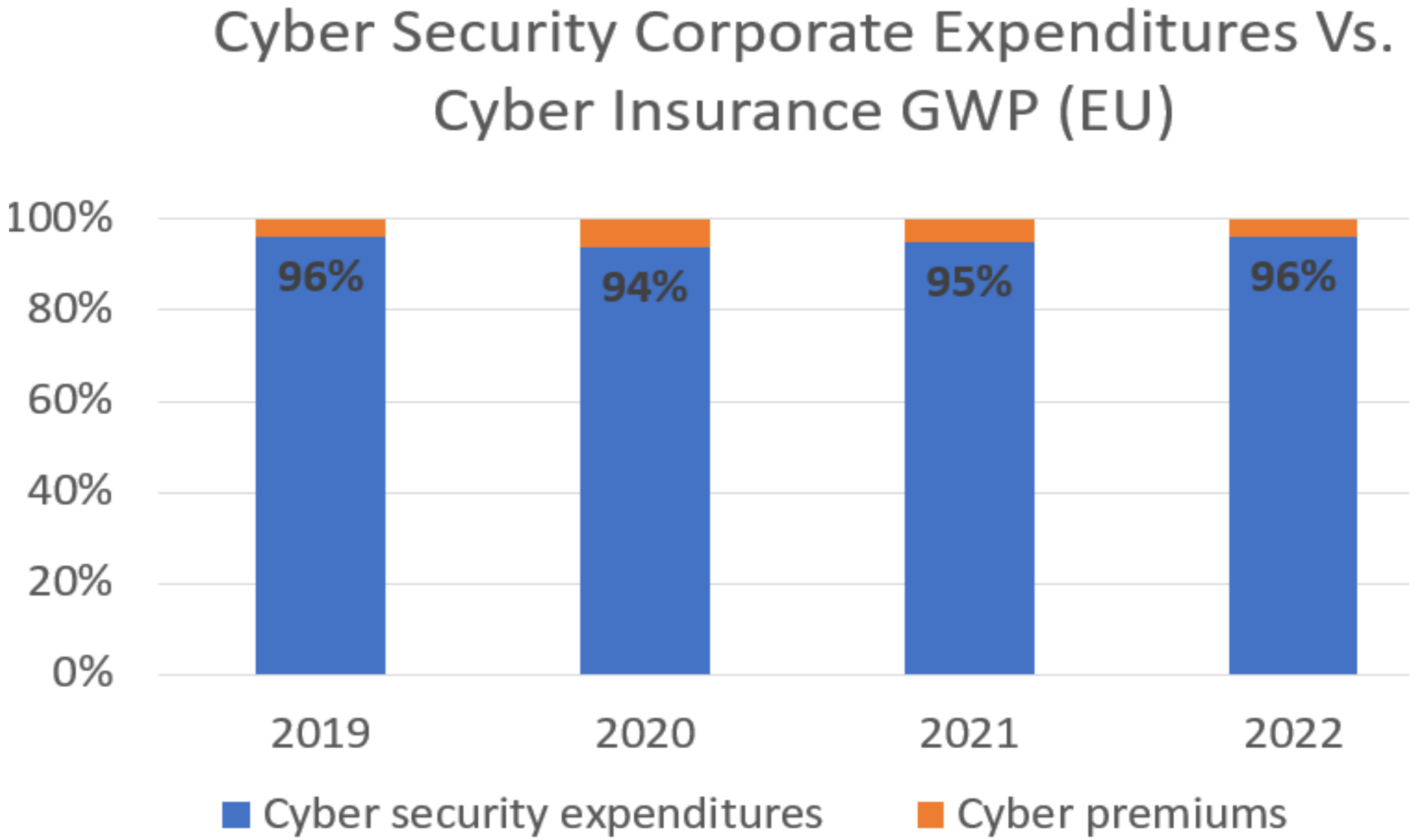

Cyber Policy Types (% of GWP, 2021, US)
24%
76%
Packaged cyber policies
Stand-alone cyber policies

Chart 3


Annual Premium Change (Renewals)
40%
20%
0%
US
EU
2019
2020
2021
2022

3. Cyber insurance – A snapshot

Chart 4



Underwriting

- Rapid technological changes shape cyber risk environment.
- There has been a significant increase in hardware and software vulnerabilities over the last few years.
- Insurers use diverse methods (usually based on external experts) to inspect the coverage offered for critical infrastructure, systemic, correlated events, and war, with some insurers restricting coverage. Evidence of proper management and controls has become critical to demonstrating cyber risk maturity to insurers.
- **The effectiveness of these methods is still to be proved.**
- Lack of relevant data and in-house underwriting expertise prohibits a reliable link between premium and cyber exposure. Underwriting remains challenging in certain industries (e.g., healthcare, IT) and countries.

Claims

- The number of cyber claims is on the rise. The COVID-19 pandemic caused an increase in cyber attacks and the geopolitical conflicts encourage cyber attacks by nations/states.
- Handling cyber claims is a complex and costly process. Measuring losses due to a cyber incident is immature and involves substantial discretion.
- In process - Insurers develop claim response and resolution models, in line with the level of claim complexity.
- Malicious data breaches are the most frequently occurring and induce the highest data breach losses.

A Unique Cyber Claim Distribution (US, 2021)

Chart 5

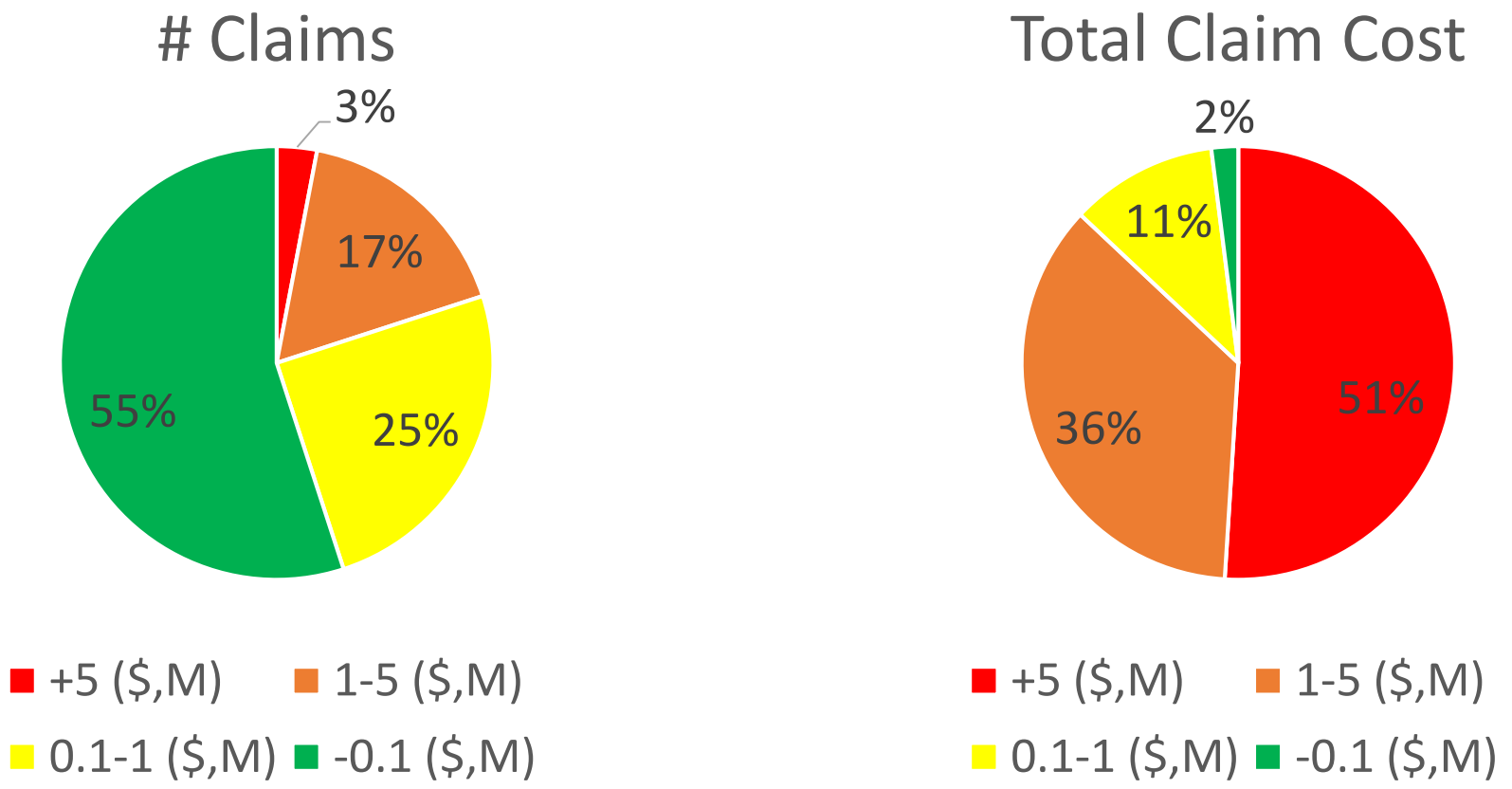


Chart 6

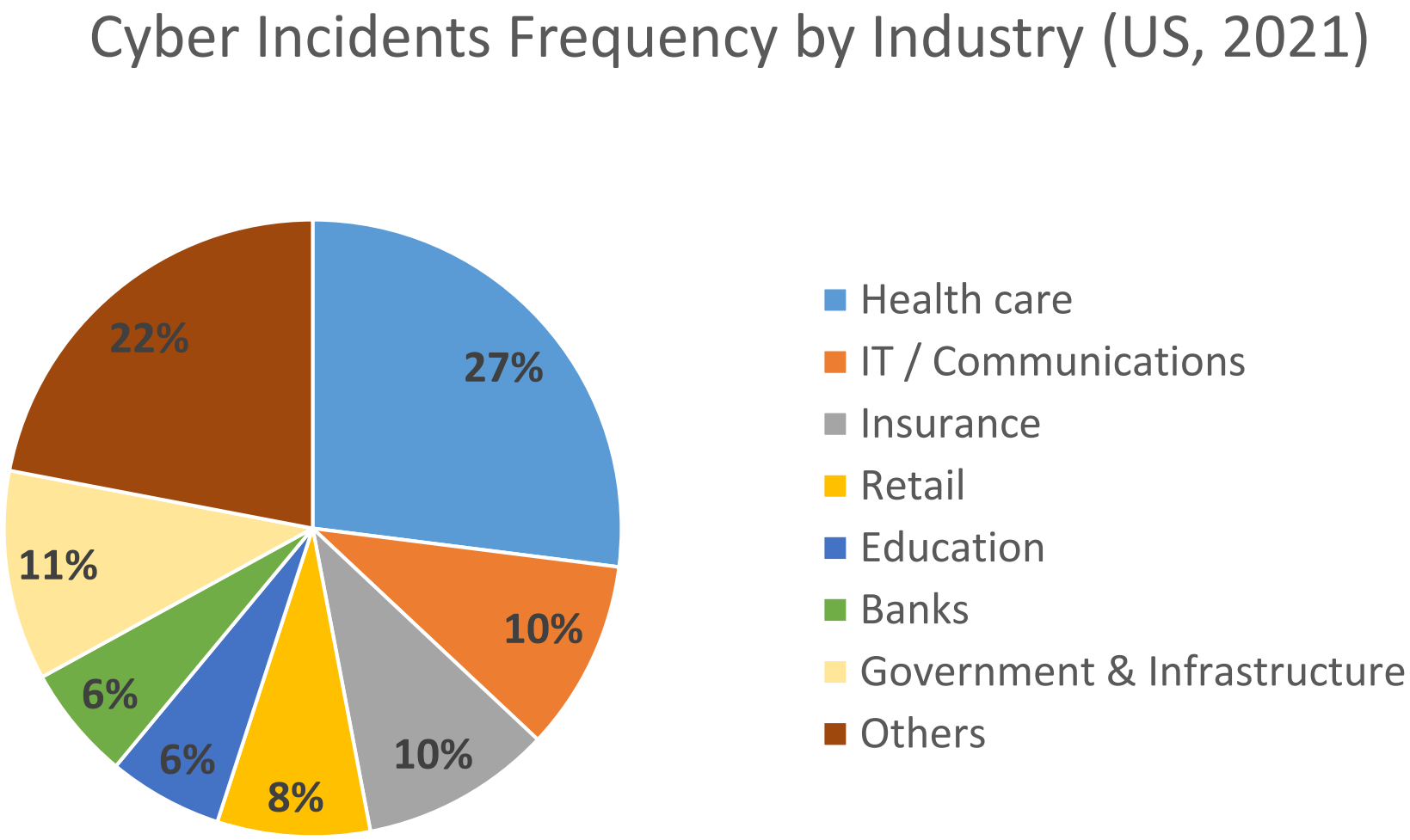

Cyber Incidents Frequency by Industry (US, 2021)
27%
10%
10%
8%
6%
6%
11%
22%
Health care
IT / Communications
Insurance
Retail
Education
Banks
Government & Infrastructure
Others

Chart 7

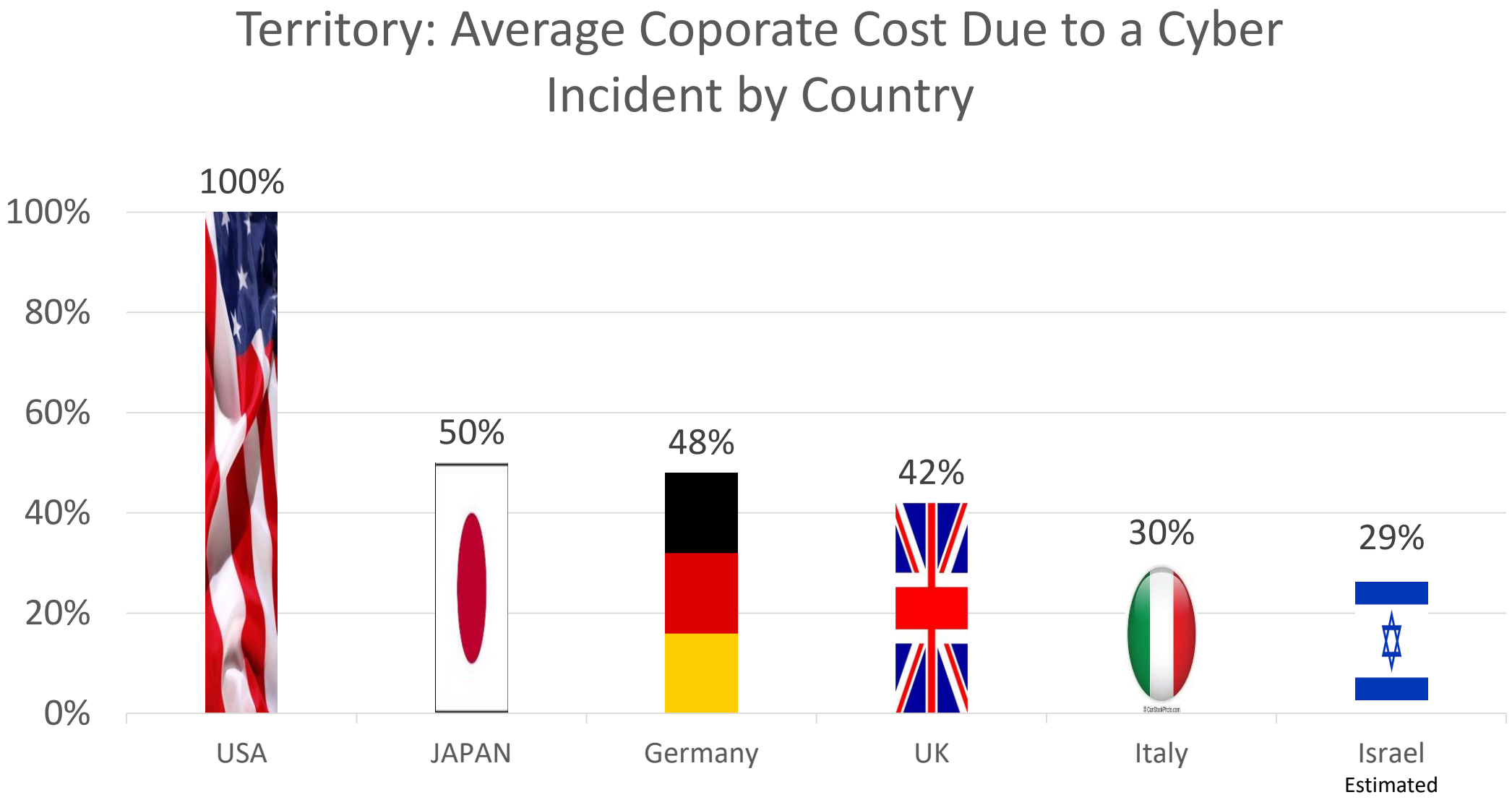
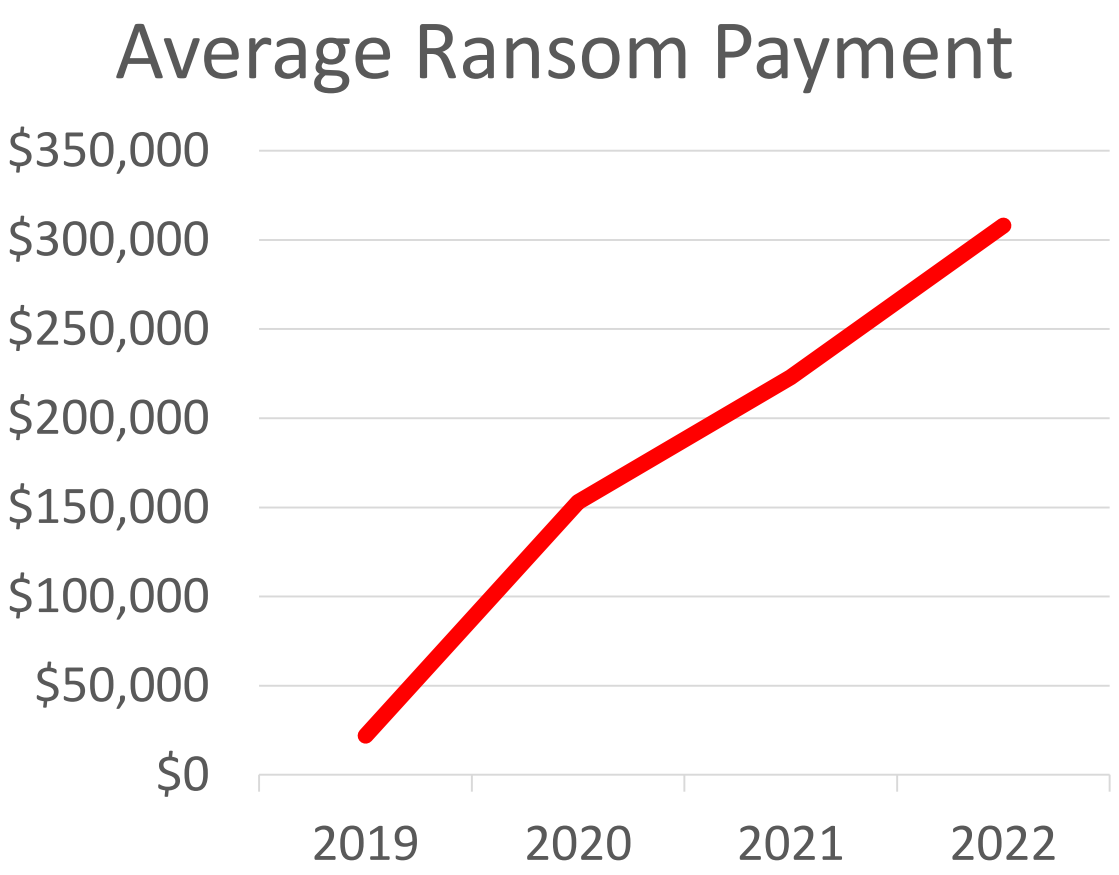
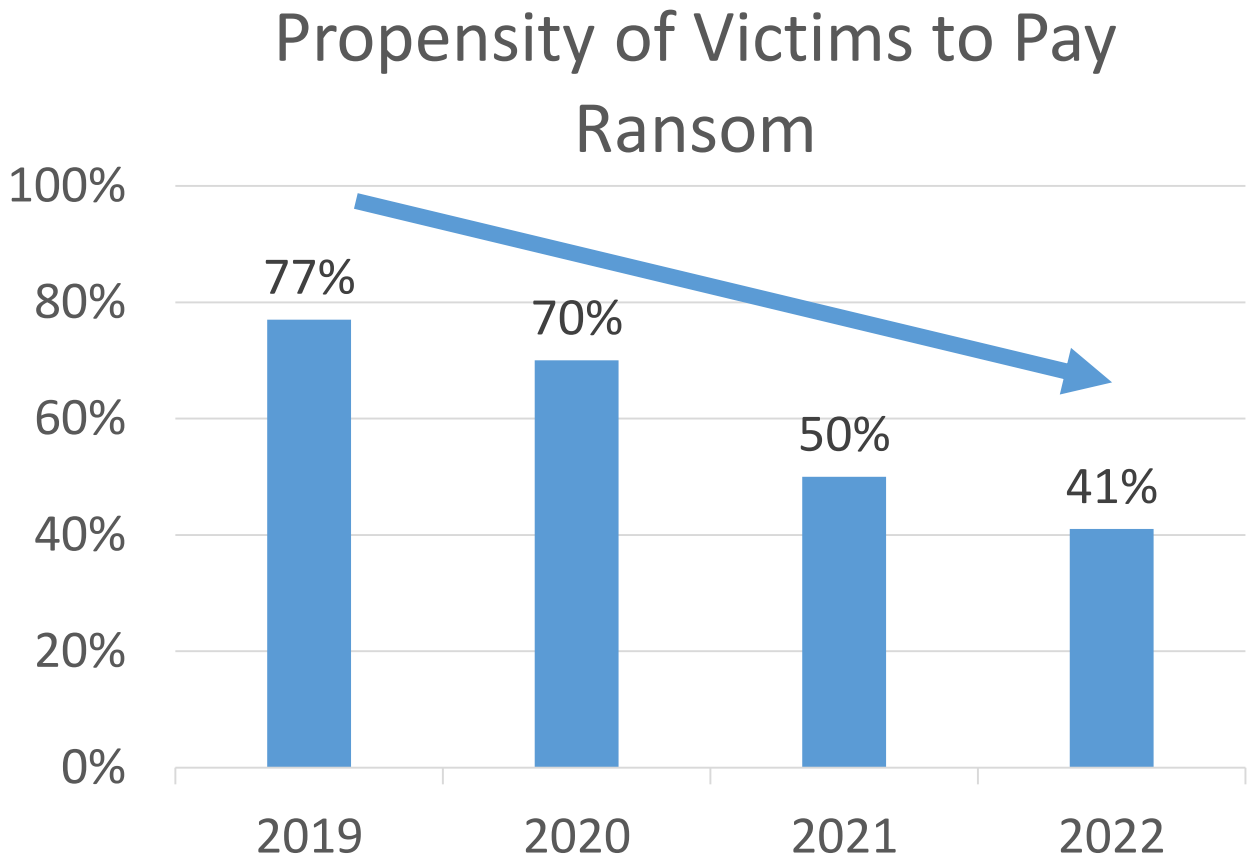

Territory: Average Coporate Cost Due to a Cyber Incident by Country
100%
50%
48%
42%
30%
29%
100%
80%
60%
40%
20%
0%
USA
JAPAN
Germany
UK
Italy
Israel
Estimated

Chart 8

A Bleary Ransom Effect

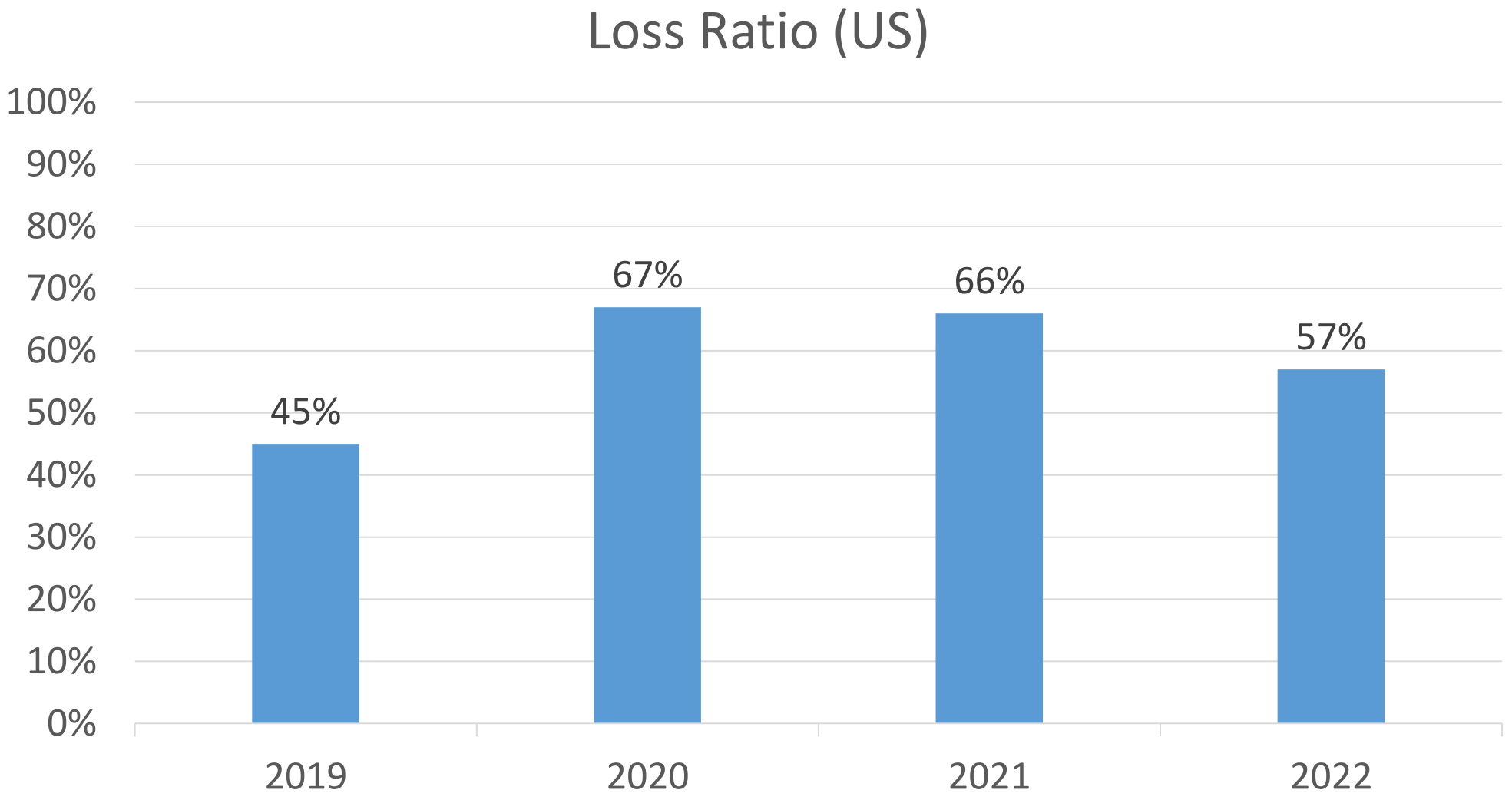




Profitability

- On average, the loss ratio of the cyber insurance segment has been highly profitable on recent years, ranging from 40% to 70% (including defense and cost containment).
- Profitability exhibits high variation among insurance firm, depending primarily on quality of underwriting.
- Insurers continue to see strong profitability, with loss ratio improvement in 2021 and 2022, due to premium rate increases and somewhat lower claims frequency.

Chart 9



Loss ratio with defense and cost containment

Reinsurance

- On average, about 45% of primary cyber insurance market premium is ceded to reinsurers (US, 2021).
- In 2021 and 2022, reinsurers offered limited cyber capacity primarily due to difficulties to predict claims.
- Increased profitability of the cyber insurance segment and limited actual losses from high profile cyber incidents raised confidence and lead reinsurers to release existing capacity constraints.
- Improved cyber security, innovative cyber modeling and the accumulation of data over time are expected to improve the ability to predict claims.
- Reinsurers take advantage of advanced technological tools at their disposal to improve the quality of underwriting and inject additional capital.

Participants in the US Cyber Insurance Market

2021 Rank	2020 Rank	Group Number	Group Name	Direct Written Premium	Loss Ratio w/DCC	Market Share
1	1	626	Chubb Ltd Grp	473,073,308	76.9%	9.8%
2	8	158	Fairfax Fin Grp	436,447,801	51.9%	9.0%
3	2	968	AXA Ins Grp	421,013,729	86.5%	8.7%
4	11	3098	Tokio Marine Holdings Inc Grp	249,785,218	43.8%	5.2%
5	3	12	American Intl Grp	240,613,748	130.6%	5.0%
6	*	3548	Travelers Grp	232,276,831	72.7%	4.8%
7	5	4942	Beazley Grp	200,877,555	38.7%	4.2%
8	7	218	CNA Ins Grp	181,382,785	87.5%	3.8%
9	*	1279	Arch Ins Grp	171,944,995	9.2%	3.6%
10	6	3416	AXIS Capital Grp	159,059,212	105.2%	3.3%
11	13	212	Zurich Ins Grp	151,865,004	76.9%	3.1%
12	14	111	Liberty Mut Grp	138,216,723	95.2%	2.9%
13	12	3219	Sompo Grp	133,519,577	54.3%	2.8%
14	10	23	BCS Ins Grp	132,043,119	80.1%	2.7%
15	*	91	Hartford Fire & Cas Grp	123,163,166	16.3%	2.6%
16	*	361	Munich Re Grp	119,989,106	69.0%	2.5%
17	20	181	Swiss Re Grp	103,827,837	32.7%	2.2%
18	*	501	Alleghany Grp	88,554,222	20.5%	1.8%
19	*	98	WR Berkley Corp Grp	81,249,260	36.9%	1.7%
20	16	31	Berkshire Hathaway Grp	71,365,401	-0.5%	1.5%
					Total	81%

Source: NAIC OCT 2022.

- There are about 6,000 insurance companies in the US. Only 570 sell cyber insurance.
- **10 (!!)** insurance groups hold **57%** cyber market share.
- **20 (!!)** insurance groups hold **81%** cyber market share.
- **6** new entrants to the top-20 list in 2021.

Terrorism Risk Insurance Program (TRIP)

- September 11 attacks resulted in approximately $50 billion of insurance losses, about two-thirds of which were reimbursed by reinsurers to insurers. Consequently, insurers and reinsurers began to exclude coverage for terrorism risk from commercial P&C policies.
- Terrorism Risk Insurance Program (TRIP, 2002) - requires US insurers to make terrorism risk coverage available within certain lines of commercial P&C insurance. Insurance losses are eligible for reimbursement through TRIP if they result from an “act of terrorism”. Cyber incidents are included.
- Two prerequisites must be met: (1) the insurer’s “insured losses” must exceed a deductible, and (2) a Program Trigger ($200 million aggregate industry level losses).
- The TRIP share is 80 percent of an insurer’s losses, subject to a cap.
- Recoupment – insurers may be required to collect funds from policyholders by placing a surcharge on ALL insurance policies written in TRIP-eligible lines.
- 80% of all commercial multi-peril (CMP) insurance policies include coverage for terrorism risk, where the incremental cost of cyber insurance is up to 3-6% of total premium.

Summary – What Do We Take-away?

- The cyber insurance segment is fast growing, profitable and highly concentrated.
- Deeper understanding of cyber exposure is in need, both on the supply and demand side, in order for the cyber insurance industry to develop further.
- Systemic and war-related cyber risks are key challenges for insurers and regulators.
- Key success factors for insurers: in-house cyber underwriting expertise, advanced technological underwriting tools and access to reinsurance capacity, generating a clear advantage to large insurers. So far, firm size and reinsurance capacity drive both market share and profitability in the cyber insurance segment.