CMS Insurance Sector Group webinar programme

Cyber

10 May 2023

Amit Tyagi (UK)
Marianna Scardia (Italy)
Tom De Cordier (Belgium)

Jorge Etreros (Spain)
Ihor Olekhov (Ukraine)
Bohdan Ilchenko (Ukraine)

Your speakers today

Amit Tyagi | Partner
T: +44 20 7367 3578
E: amit.tyagi@cms-cmno.com

Tom De Cordier | Partner
T: +32 2 743 69 13
E: tom.decordier@cms-db.com

Ihor Olekhov | Partner
T: +38 044 391 3377
E: ihor.olekhov@cms-cmno.com

Marianna Scardia | Associate
T: +39 02 8928 3800
E: marianna.scardia@cms-aacs.com

Jorge Etreros | Senior Associate
T: +34 91 452 00 32
E: jorge.etreros@cms-asl.com

Bohdan Ilchenko | Associate
T: +38 044 391 3377
E: bohdan.ilchenko@cms-cmno.com

What we will cover

01 Cyber insurance in Ukraine: Market and Prospects

02 The evolution of incidents and claims handling

03 Regulatory changes and impact of the conflict

04 Evolution of the cyber risk in Italy and beyond

05 Forecast for the future

06 Q&A

1 Cyber Insurance in Ukraine: market and prospects overview

Current insurance market overview

127

There are 127 registered insurance companies on the Ukrainian market:

115

non-life insurance

12

life insurance

In accordance with the latest official statistics from the National Bank of Ukraine the total assets amount of the insurers in Ukraine is:

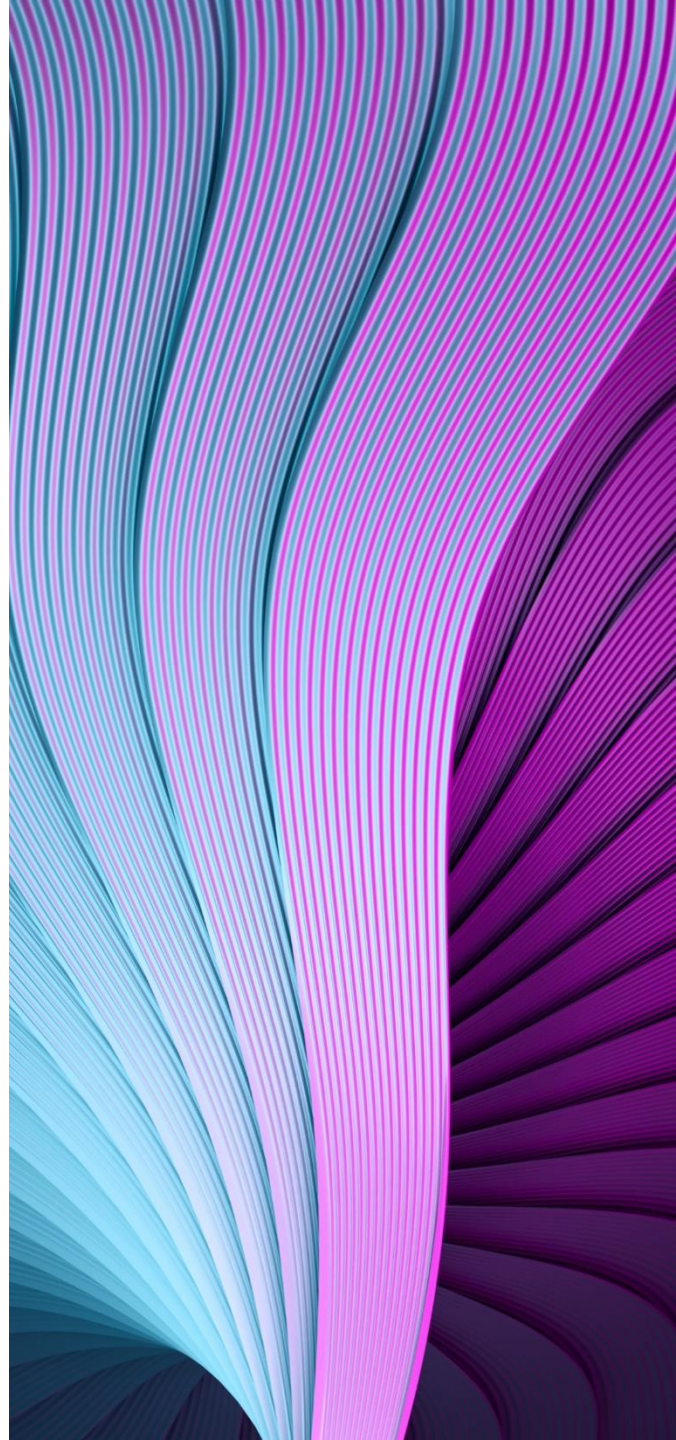
65,7 billion UAH

Many insurers in Ukraine are **actively using digital tools like Apps and cooperating with other leading financial institutions** (e.g. Monobank) to promote and distribute their insurance services

Current insurance market overview

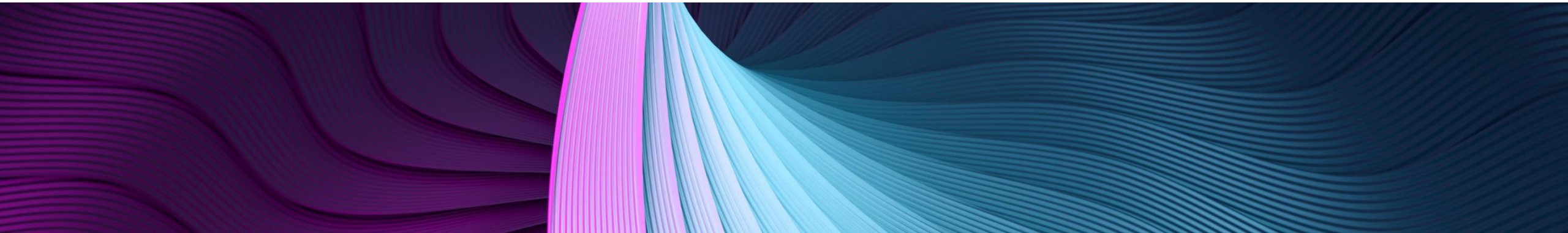
The insurance market in Ukraine is temporarily experiencing difficult times. The difficult situation on the insurance market in wartime encourages small insurance companies to merge with market leaders. But practice shows that in some cases even insurers with large and diversified portfolios may not be able to withstand difficulties: the regulatory ratios are still in force and must be strictly complied with.

In total, 17 insurance companies have been withdrawn from the market since the beginning of the full-scale war.



However, the insurance market has prospects of real growth in the near future. The economy is recovering, and insurers are adapting to the new conditions: some of them have even grown significantly in 2022.

The most difficult stage has already been passed, so 2023 will be characterized by an improvement in the market situation.



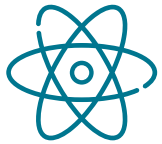
Cyber insurance is not an exception:

The development of technologies and the growing number of cyberattacks (especially from Russia) make this area extremely relevant.

More and more insurance companies are expanding their range of services to cover cyber risks.

Financial companies may face significant risks from cyberattacks, which are among the most substantial threats they may encounter.

These risks can encompass a range of potential hazards, including:



DDoS attacks

Hacker attacks

Virus attacks

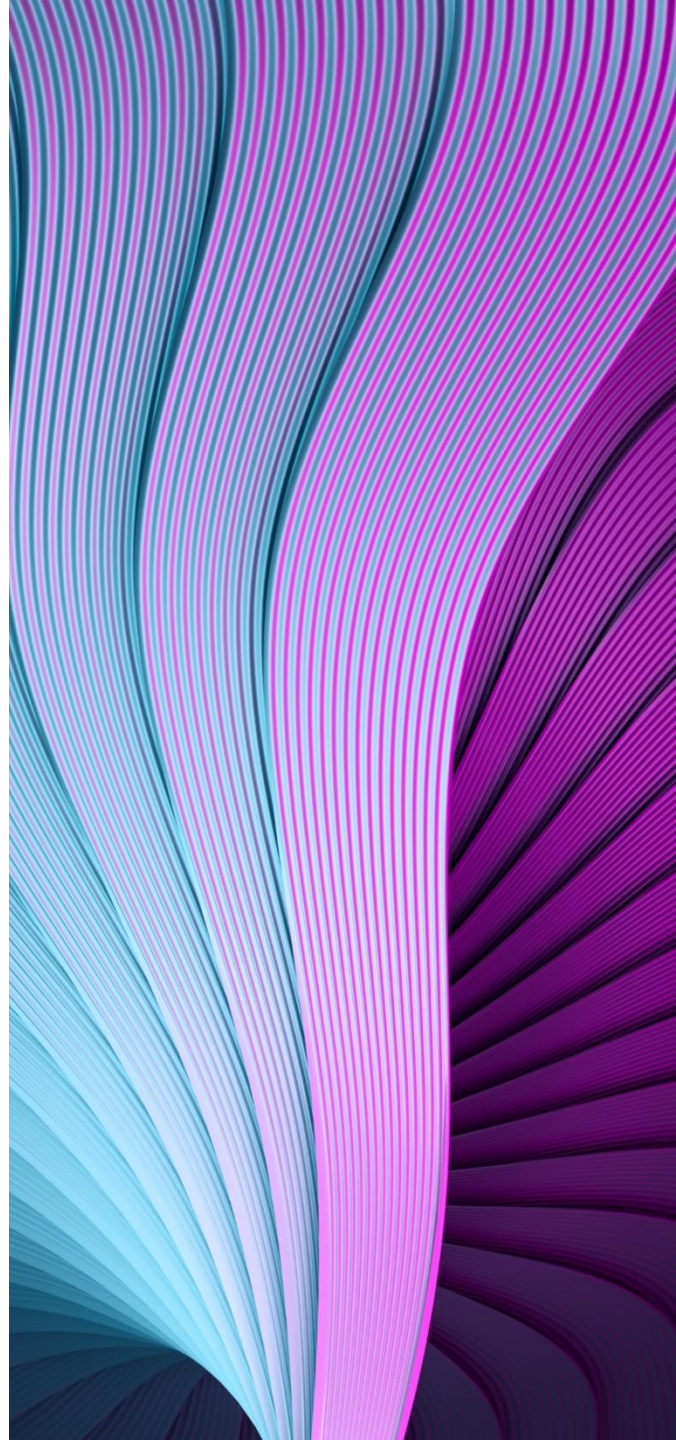
Ransomware

Phishing etc.

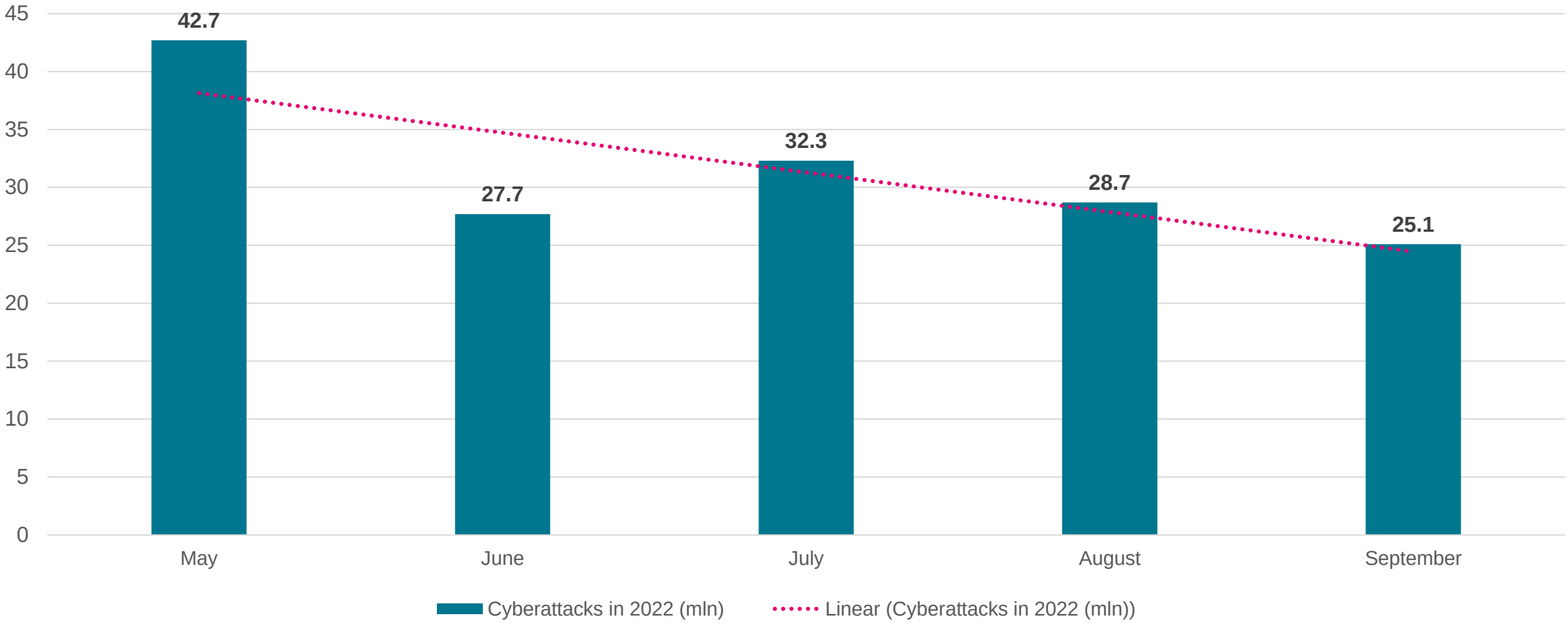
Growth of frequency of cyberattacks against financial sector

Over the past ten years, the number of cyberattacks has increased significantly. A key role in this has been played by Russia, which regularly engages in aggressive actions in cyberspace against Ukraine and private institutions. 2022 was a peak year in this regard: according to the State Connection Service, the number of attacks in May-September 2022 averaged 31.3 million per month.

Financial companies are one of the primary victims among the impacted parties. This is eloquently evidenced by the data not only of the State Connection Service, but also of the financial services market participants themselves: in particular, Sense Bank reported that the number of attacks in 2022 increased by 800-1000 times compared to previous years.



Cyberattacks in May – September 2022 (mln)



At the same time, foreign partners help Ukraine to fight on the cyber front:

The **U.S.** has invested more than $40 million in Ukrainian cyber defense since 2017 and regularly advises government agencies on countering Russian intelligence services

The **U.K.** compensates Ukraine for the services of private cyber defence companies

NATO admitted Ukraine to its Cooperative Cyber Defence Centre of Excellence

Microsoft, Google, AWS, Cloudflare and a number of other IT giants helped Ukraine to transfer databases of state bodies and enterprises to the cloud, and also provided free access to them and much more

How to mitigate the risk of cyberattacks

One of the effective ways to mitigate the risk of incurring large losses due to a cyberattack is cyber risk insurance. Depending on the insurer, it may cover, in particular, the following:

Direct losses from business interruption, data leakage, the need for repair works.

Damages to third parties – liability for data leakage or theft of currency values.

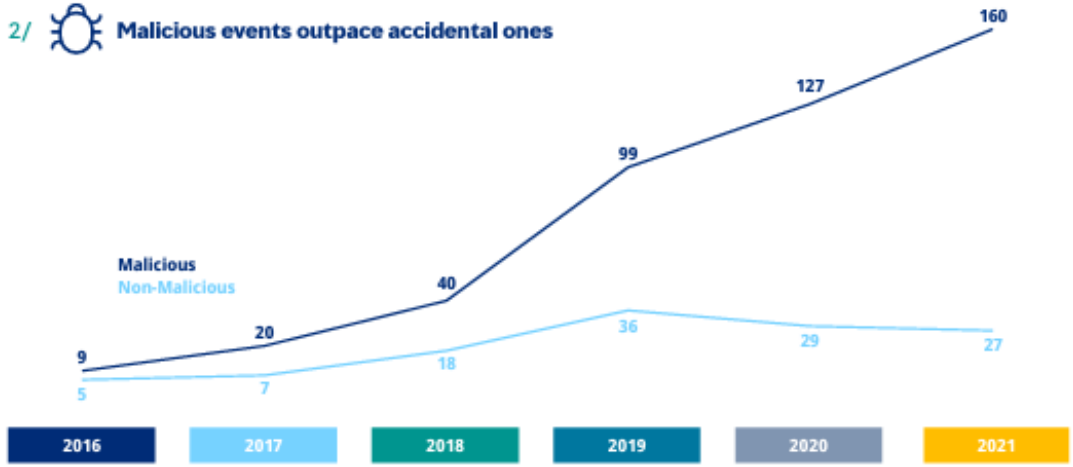
Legal aid and court representation costs.

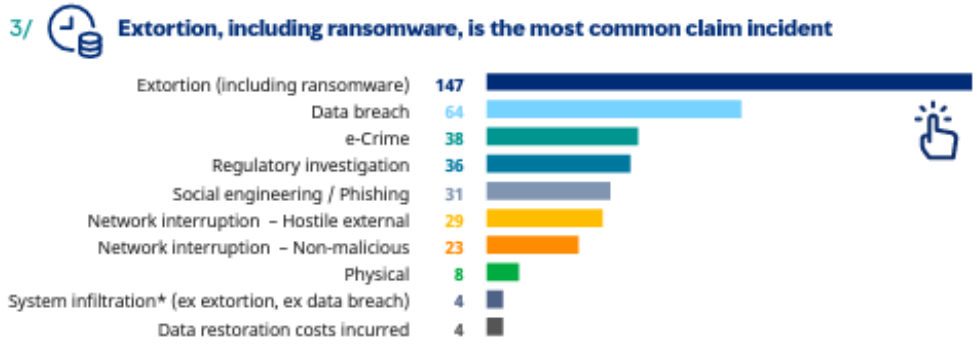
Expenses for expert and advisory support.

2 The evolution of incidents and claims handling

Evolution in incidents

- Increase in malicious events
- Greater severity and sophistication
- Evolution in ransom attacks
- Increase in phishing attacks and payment fraud

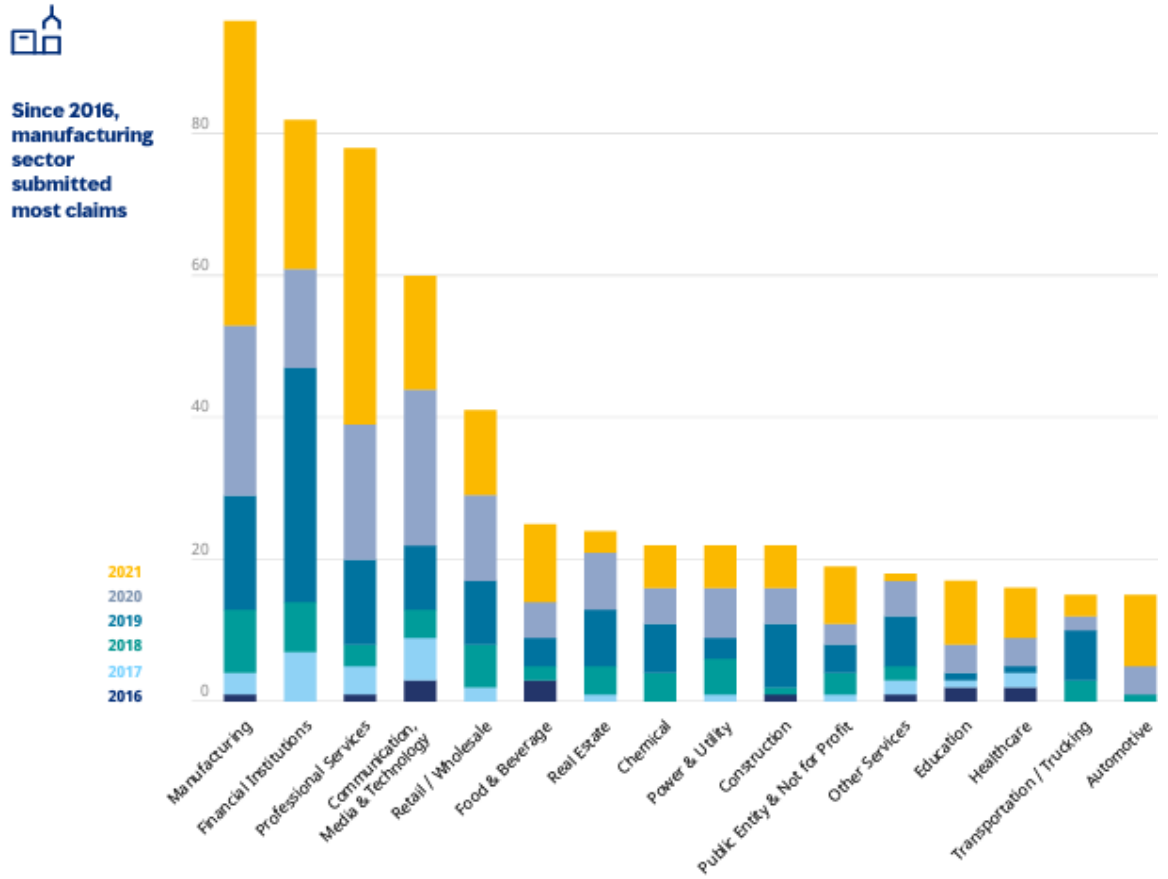




Source: The Changing Face of Cyber Claims 2022

Evolution in incidents – Sectors attacked 2016-2021

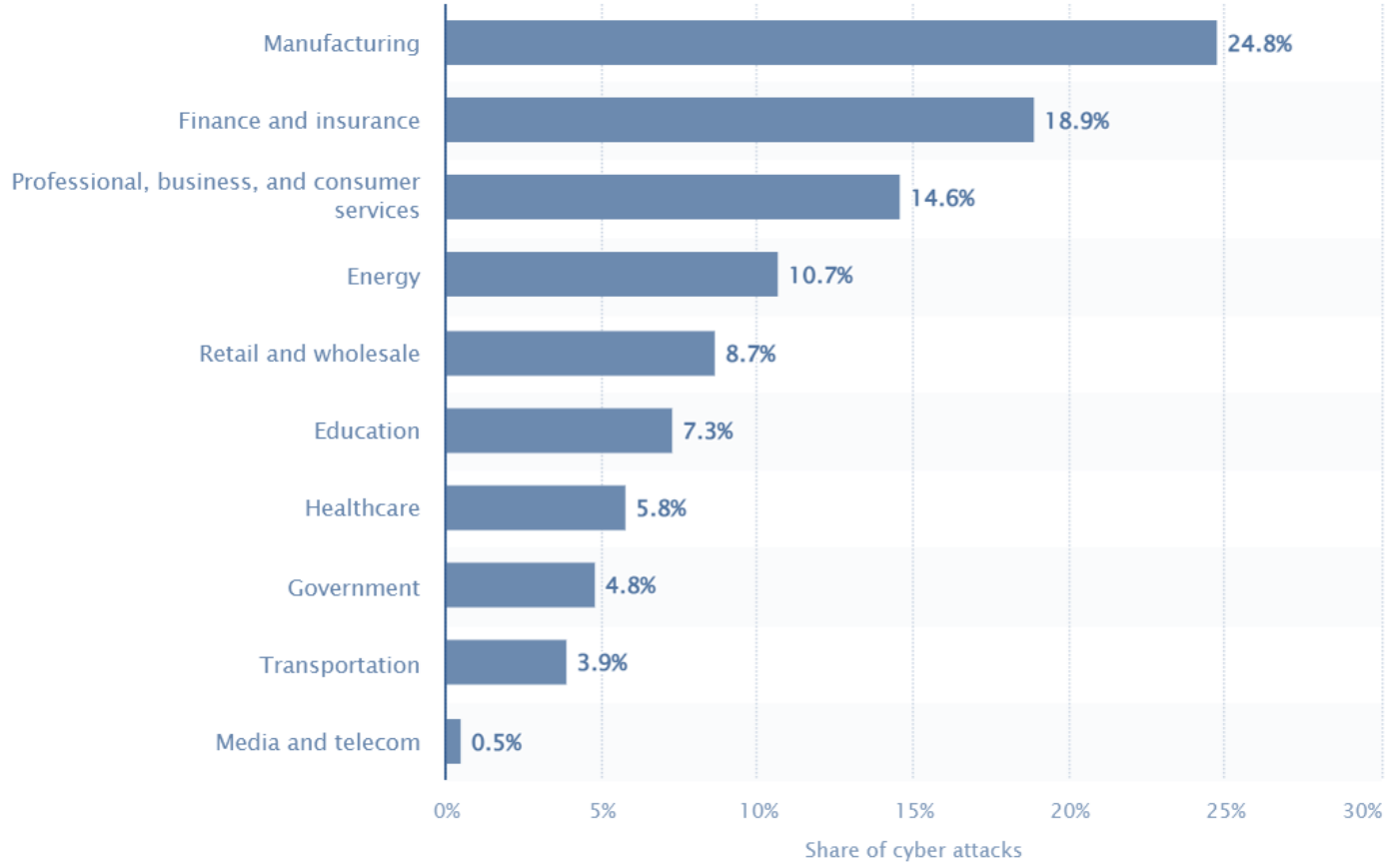
- Manufacturing sector a key developing target
- Financial and professional services remain key targets
- Digitalization of all companies implies greater risk.



Source: The Changing Face of Cyber Claims 2022

Evolution in incidents – Sectors attacked in 2022

- Significant increase in 2021 and 2022 in healthcare. Vulnerability due to sensitive personal data and operational risk
- Focus on education
- Eyes on Goverment and energy (oil and gas).



Source: The Changing Face of Cyber Claims 2022

Evolution in handling of incidents

- Lessons learned
- Increased knowledge of participants
- Explosion of service providers – pool of experts
- Times and costs estimations
- Quicker responses vs quicker solutions
- New collaterals: associated legal work, civil claims from contractual partners and recovery claims against third parties.

Examples of incidents

Data **exfiltrated** & **cryptolocked** with request to pay ransom in virtual currency.

APT: State-sponsored hack (originating from rogue state) + exfiltration of intellectual property.

Email spoofing

↓

Purchase price for recent acquisition was wired into fraudulent bank account.

Hack into mailbox of senior management

↓

strategic information about confidential **M&A transaction** potentially exposed.

Threat by **disgruntled temporary worker** whose contract was not extended.

IT-consultant published **scripts on Github** (public directory) containing **security credentials** which have been used by a Chinese IP address to intrude into IT environment.

Do’s & don’ts based on our real-life experience – **DO’S**

- **Call** the insurer’s or broker’s **hotline** asap (even if unclear whether incident is covered by policy)
- Be mindful of **confidentiality**: only disclose the incident to those that have a strict need to know
- Consider **legal privilege**: when involving external forensic experts you may want to contract them through external counsel to vest legal privilege in the findings of the experts
- For **fast and confidential communication** between all the various stakeholders (internal IT; internal CISO; external forensics; external counsel; other stakeholders) consider setting up a dedicated group in Signal, Threema or Whatsapp
- Set up **daily status update calls** with all involved stakeholders (internal IT; internal CISO; external forensics; external counsel; other stakeholders)
- **Document** the incident + actions undertaken to remediate and improve (including severity assessment)
- **Manage** and **monitor** your external service providers (e.g. audit; e.g. ISO 27018 certification).

Do’s & don’ts based on our real-life experience – **DON’TS**

- **Over-enginee**r (e.g. do not make your IR procedure complex)
- **Shut down hardware** that is affected (just isolate it from the internet/network) – **Talk to the experts**
- **Underestimate** the amount of **effort & time** you will need to solve a cyber attack (marathon vs sprint)
- Be narrow-minded. Handling a cyber attack requires a **multi-disciplinary approach** (IT, CISO, Legal, Comms, Insurance, senior management, etc.).
- Forget to solve the **weak spots**:
  - Roll out MFA (on all accounts)
  - Promptly patch vulnerabilities
  - Roll out state of the art EDR (Sentinel One, Crowdstrike Falcon, etc.)
  - Run internal training & awareness-raising campaigns
- **Don’t waste a good crisis.** Use incident to define and implement improvements to your systems/ processes.

3 Regulatory changes and impact of the conflict

Regulatory changes affecting incidents

- Network and Information Systems (NIS):
  - **EU:** NIS 2 Directive entered into force on January 2023
    - Stricter obligations on risk management, incident reporting and information sharing
    - New obliged subjects
    - Essential sectors: energy, transport, banking, healthcare, government, etc.
  - **UK:** UK GDPR, no direct application of NIS2 but enhancements to UK NIS
- Digital Operational Resilience Act (DORA)
- Data protection rules
- Class actions
- Ransomware payment

Impact of the conflict on handling incidents

- Initial decrease of incidents following invasion: Theories behind this
- Phishing campaigns against Ukraine
- Now back to “normality”
- Ransomware payment: US and EU sanctions, SWIFT exclusion, etc.
- Attacks to NATO partners
- Cryptocurrencies.

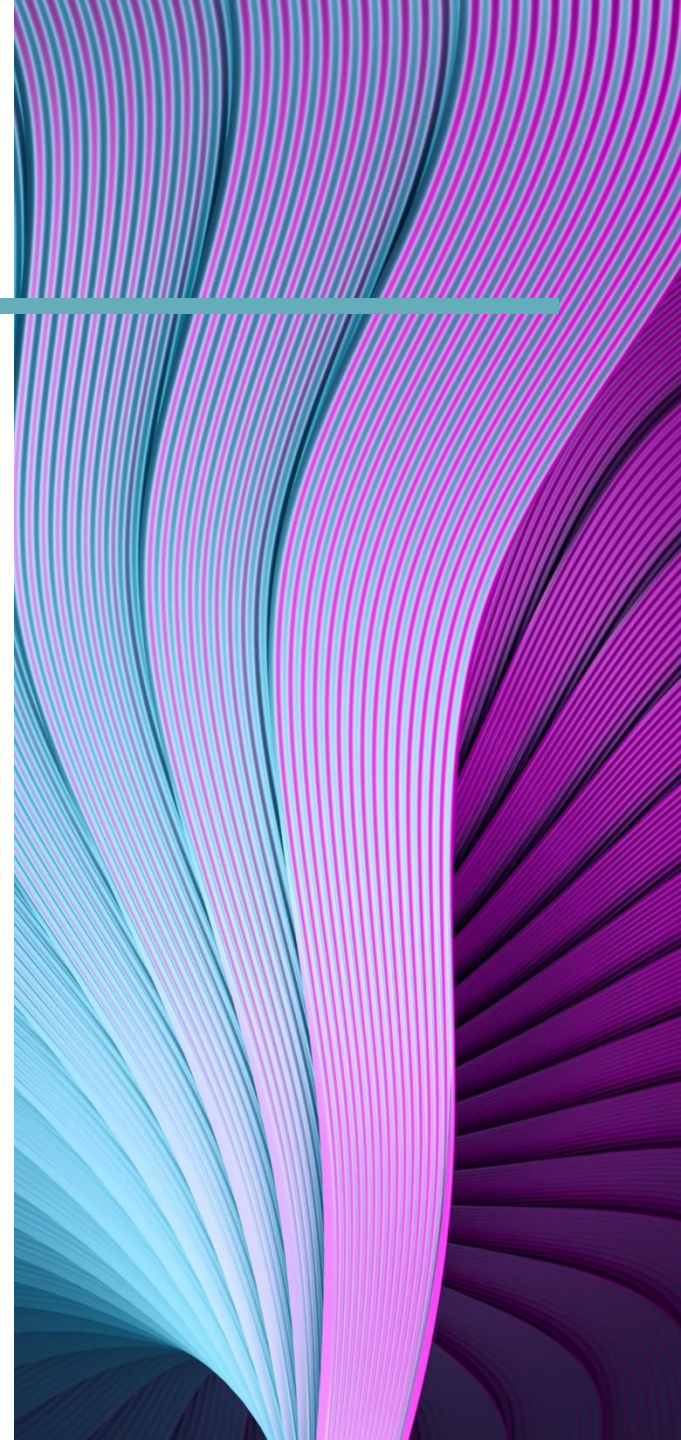
4 The evolution of the cyber risk in Italy and beyond

The cyber risk in the Italian market

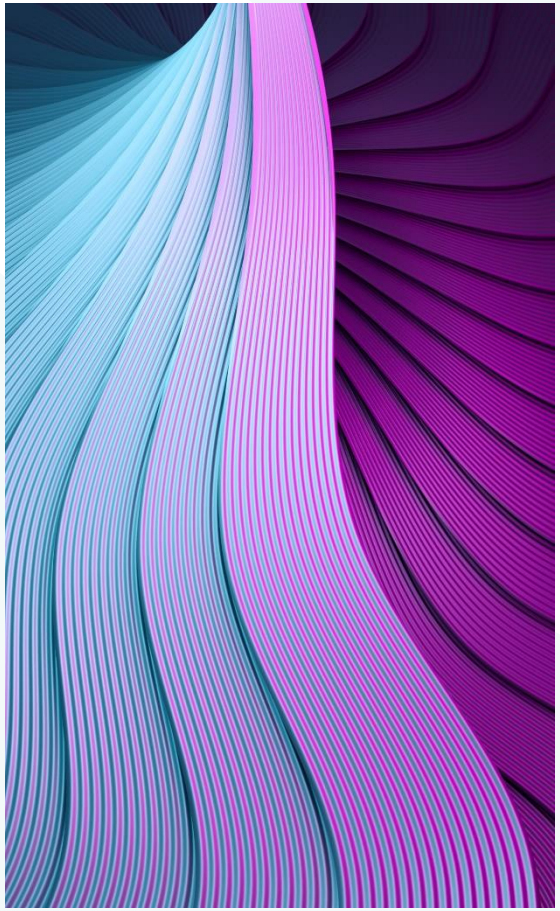
- Cyber incident (e.g. cyber crime, malware/ransomware causing system downtime, data breaches, fines and penalties) and business interruption (incl. supply chain disruption) are the **top two business risks for 2023**
- The risk related to cyber incident and business interruption **impacts on companies of all sizes** (e.g. a significant number of cyber incidents involves small manufacturing companies).

Legal framework

- GDPR and Privacy code
- Trade secret legislation
- Criminal law
- Cyber security legislation
- Banking, finance and insurance law
- Civil law



Legal evolution on cybersecurity and prevention of cyber risks



DORA Regulation

- ✓ Published in EU journal in **December 2022**
- ✓ Entry into force: **17 January 2025.**

NIS 2 Directive

- ✓ Published in EU Journal in **December 2022**
- ✓ It repealed NIS Directive implemented in Italy by Legislative Decree 65/2018
- ✓ Not yet implemented.

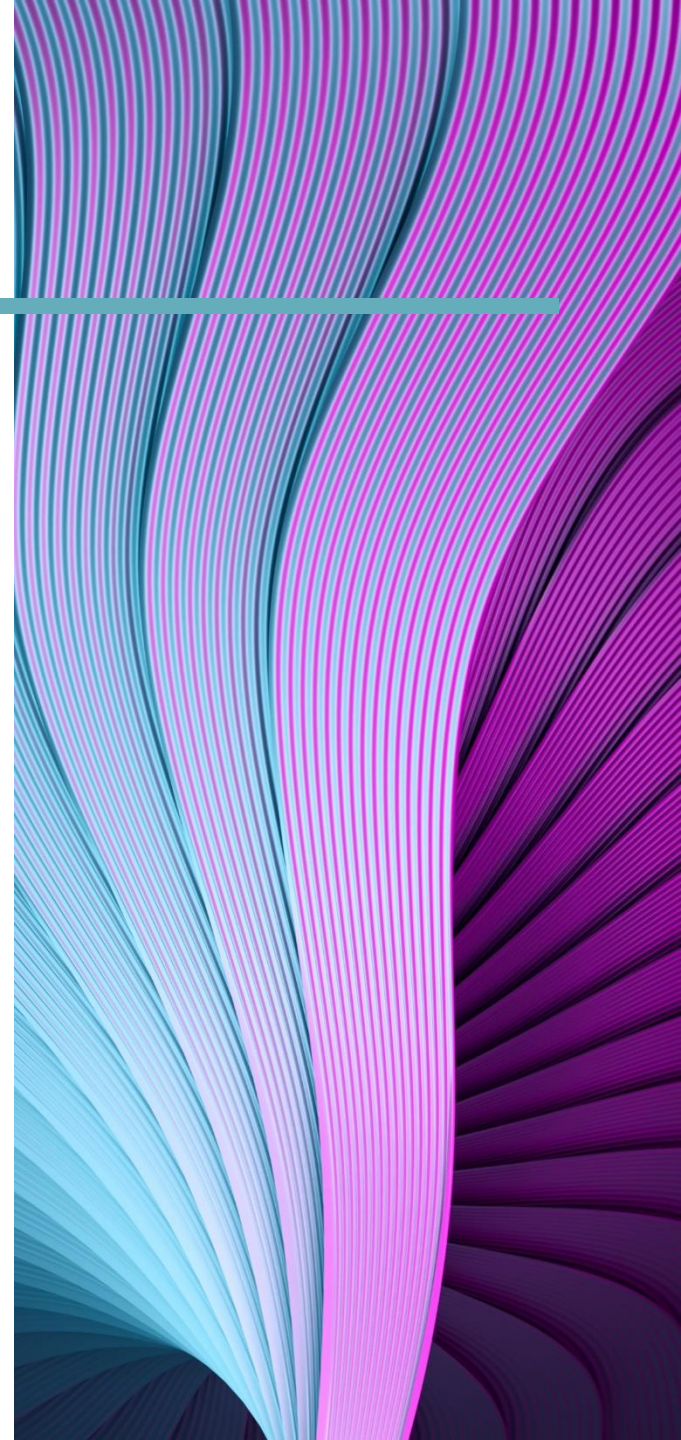
Potential impact of a cyber incident: indemnifiable losses

- Reputational risk and impairment of customer relations
- Risk of compensation of damages suffered by third parties
- Business interruption
- Data breach and breach of trade secrets

Cyber policies: potential issues in the underwriting process

Correct identification of the risk:

- the concept of systemic risk
- the need for technical support
- the “continuous monitoring” of the risk.



Cyber policies: most frequent coverage issues

Correct identification of the loss for business interruption:

- Time allocation of the loss (maximum indemnity period, time deductible)
- Costs to be reimbursed (different allocation of workers for the management of the intervention).

The war exclusion: should it be reconsidered?

- The war exclusion excludes coverage for losses resulting from a war
- Nowadays conflicts have a strong impact on cyber world. Before the the launch of the “Special military operation” in Ukraine, it had been identified that cyber attacks would be a key component of any future conflict
- Cyber policies contain the war exclusion like any other policy
- This exclusion must be rethought since it does not fit with modern times
- NB Lloyd’s war exclusions are the subject of much debate

5 Concluding remarks & forecast for future

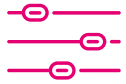
Forecast for future

Greater uptake in standalone cyber insurance policies.

“Inside-out” underwriting focus but uncertainty remains.

Continued rise in claims costs.

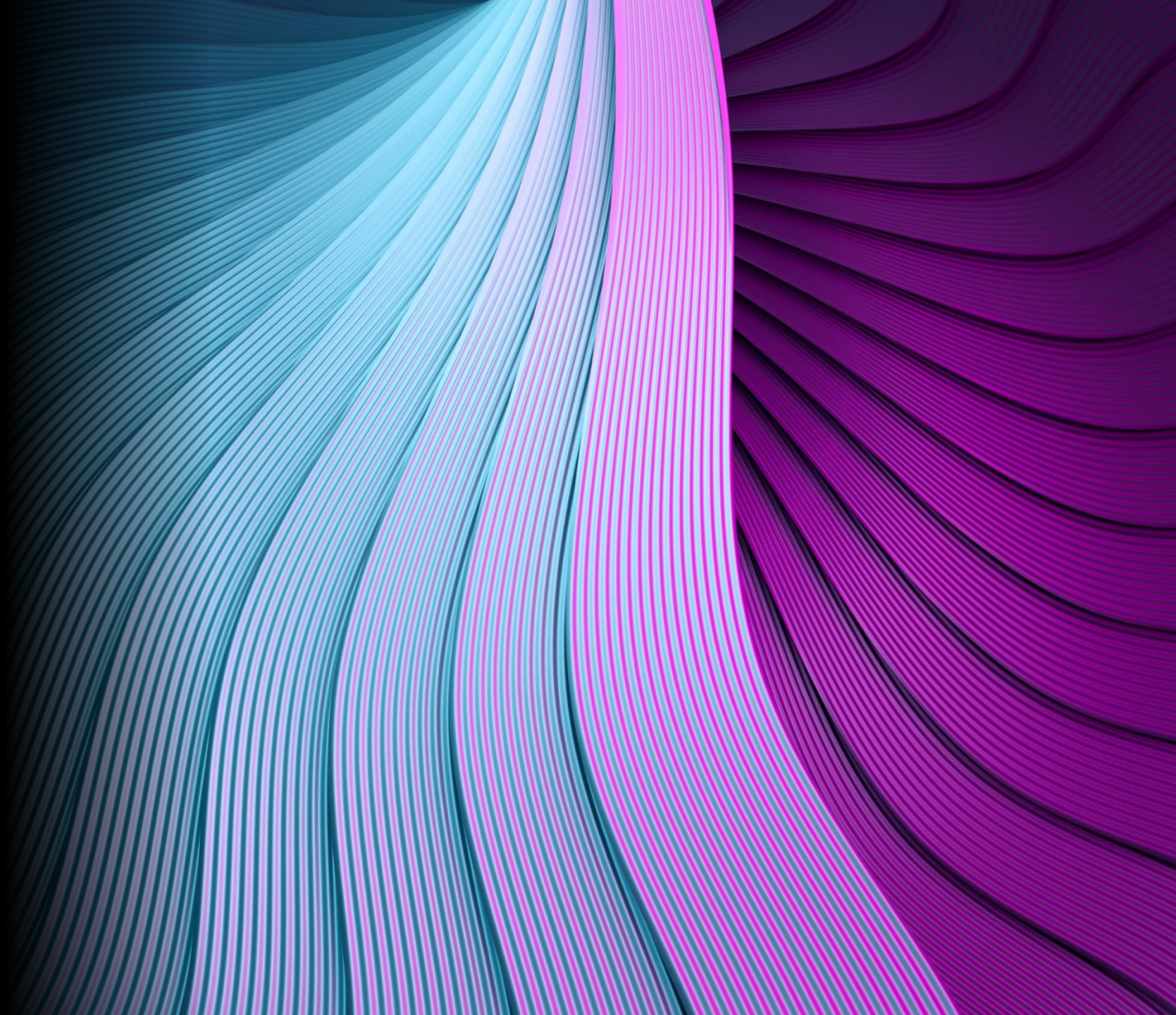
Aggregation risk for insurers / reinsurers.



Difficult coverage issues for the market.

Increasing willingness of insurers to take coverage points?

Questions?



CMS Law-Now™

Your free online legal information service.

A subscription service for legal articles on a variety of topics delivered by email.
cms-lawnow.com

CMS locations:
Aberdeen, Abu Dhabi, Algiers, Amsterdam, Antwerp, Barcelona, Beijing, Belgrade, Bergen, Berlin, Bogotá, Bratislava, Bristol, Brussels, Bucharest, Budapest, Casablanca, Cologne, Cúcuta, Dubai, Duesseldorf, Edinburgh, Frankfurt, Funchal, Geneva, Glasgow, Hamburg, Hong Kong, Istanbul, Johannesburg, Kyiv, Leipzig, Lima, Lisbon, Liverpool, Ljubljana, London, Luanda, Luxembourg, Lyon, Madrid, Manchester, Mexico City, Milan, Mombasa, Monaco, Munich, Muscat, Nairobi, Oslo, Paris, Podgorica, Poznan, Prague, Reading, Rio de Janeiro, Rome, Santiago de Chile, Sarajevo, Shanghai, Sheffield, Singapore, Skopje, Sofia, Stavanger, Strasbourg, Stuttgart, Tel Aviv, Tirana, Vienna, Warsaw, Zagreb and Zurich.

---

cms.law