2024 Insurance Sector
Webinar Programme

Managing an international cyber incident: Perspectives from the UK, EU, South America and Asia

29 May 2024

Moderator:
Amit Tyagi (UK)

Panel:
Leonard Böhmer (CMS Netherlands)
Sheena Jacob (CMS Singapore)
Felipe Bastos (FAS Advogados in cooperation with CMS, Brazil)
Danilo Weiller Roque (FAS Advogados in cooperation with CMS, Brazil)

Your speakers today

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

Leonard Böhmer | Partner
T: +31 20 301 62 48
E: leonard.bohmer@cms-dsb.com

Sheena Jacob | Partner
T: +65 6422 2851
E: sheena.jacob@cms-holbornasia.com

Felipe Bastos | Partner
T: +55 11 3805-0222
E: fbastos@fasadv.com.br

Danilo Weiller Roque | Associate
T: +55 11 3805 0222
E: droque@fasadv.com.br

What we will cover

01 Preparing for an incident

02 Managing an incident

03 Long tail issues

04 Questions

Extensive Global Cyber Network

- CMS offers seamless support in over 50 jurisdictions as part of our global breach response network outlined in the map.

We also work with a number of trusted local firms on international cyber incidents and have a well-developed network with whom we have built strong relationships.

"Having been one of the early firms to create a global incident response service, that service is now one of the best we use. It operates seamlessly to provide global advice in short time frames and without incurring massive costs."

Legal 500, Data Protection and Cybersecurity

1 Preparing for an incident

Preparing for an incident

Europe

- ”One stop shop” in multiple jurisdictions: Regulatory authority of the main establishment has the lead both in the receipt of notifications and the conduct of investigations
- Which regulatory authority? Data protection or special authority (financial services)
- Other entities or bodies (external and internal)?
- Language issues and cultural issues
- Disaster and recovery plan? Exercise?
- NIS2 and other upcoming rules and regulations?
- Cyber risk awareness training (pen tests and trainings)

Full harmonisation vs. local laws

Europe

Frequent assumption:

- Legal framework is largely or even fully harmonised

Reality:

- GDPR: Full harmonisation as general concept
- 'Opening clauses' permit deviations in member states
- Moreover: Relevance of local laws in, e.g., enforcement: data protection authorities act on the basis of GDPR and local (administrative/procedural) law
- Same local law relevance re: GDPR damage claims: local courts apply GDPR and local procedural law

Preparing for an incident

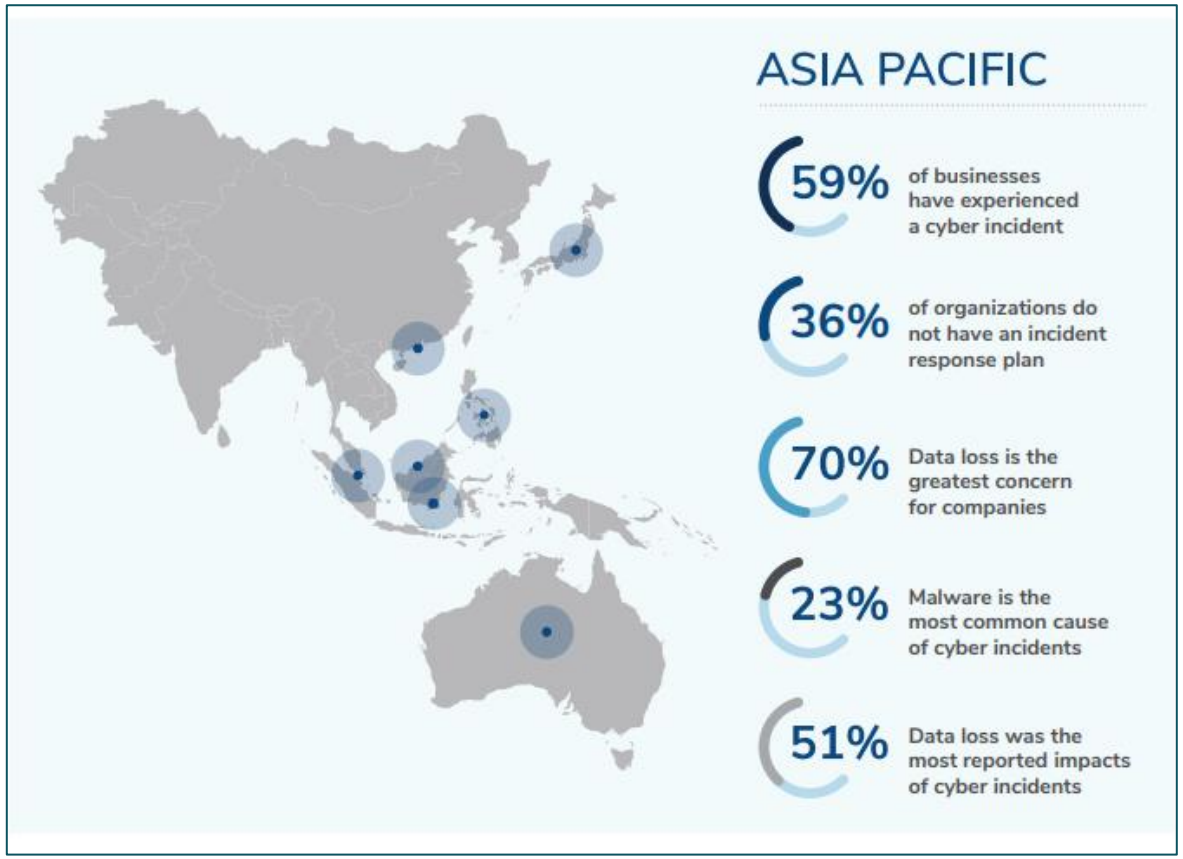
South America

- LatAm suffered 12% of global cyberattacks (vs. 8% of the world's population)
- One of the most vulnerable regions to cyberattacks – while it is in the 6th place amongst those that have invested on cyber security capabilities (above Africa and Oceania only)
- Brazil is the 2nd country most vulnerable to cyberattacks in the world and ranks 3rd as the country which suffered most cyber attacked (6%). Mexico runs in 6th, Chile in 8th and Peru in 10th
- Brazil leads ransomware cases in Americas – even ahead of the USA

Preparing for an incident

Asia

2022 Outlook for APAC



Source: Kroll APAC 2022

2 Managing an incident

Managing an incident

Europe

- Language issues and cultural issues
- Role of the IT-provider
- When to notify potentially affected persons (legal obligation/matter of courtesy/pr
- Are you allowed to pay ransomware? (Trend: rather not)
- The trending obstruction by the banks (and their Anti Money Laundering protocols)

Preparing for an incident

South America

12 countries: 7 with data protection laws

Mandatory Report to DPA

- 5 jurisdictions – from 48h to 15 days
- Argentina: DPA and EU adequacy decision – no mandatory reporting (pending legislation could change this)
- Brazil: mandatory notification by controller to DPA under a predefined format, and system for notification 3 business days. Not every incident must be reported.
- Chile: no DPA, no report required
- Uruguay: 72 hours to report to DPA – includes legal entities data

Notification To Data Subjects

- Brazil (3 business days)
- Ecuador (2-3 days)
- Uruguay (ASAP)
- Peru and Panama (immediately)
- Mexico (promptly): mandatory
- Colombia: good practice

Notification To Other Bodies

- Varies widely
- Usually highly regulated sectors (e.g. SEC, health, and banking) or critical infrastructure/services (e.g. telecom, electricity)

PENALTIES

Range from administrative warnings to fines and operational closures, with fines up to USD 10MM in Brazil for severe breaches.

Managing an incident

South America

Challenges and Best Practices

- No one-size-fits-all solution: independent legal and procedural landscapes
- Key t\o act swiftly and effectively; earlier identification, interruption, and remediation can mitigate impact
- Careful evidence collection is crucial
- Notify the insurer (when applicable)
- Small number of local incident response service providers

Ransomware Considerations

- Brazil: prone to paying ransoms, does not prohibit ransom payments
- Payments do not guarantee recovery and may encourage future attacks; studies show high rates of re-victimization and additional payment demands

Regulatory Approach

- Regulators have a tendency to punish
- Prior diligence and good faith during the incident response are usually taken into consideration (mitigating circumstances)

Managing an incident

Asia

Notification to Regulators

Source: MapChart

3 Long tail issues

The long tail of an incident

South America

Claims Landscape

- Individuals can generally file for property/economic and moral damages in all jurisdictions, but damages are not presumed
- Accessibility of mass/class actions varies from country to country; more restricted in Peru, more accessible in Brazil

Special Litigation Concerns in Brazil

- High litigation culture, low cost, and accessible justice system raise concerns, especially under LGPD (General Data Protection Law)
- Recent trends show courts siding with companies where mere incidents do not necessarily result in liability for damages

Future trends

- Increased cyber-diplomacy and cooperation (e.g. OAS Cybersecurity Program)
- Implementation/improvement of local and regional cyber strategies
- Increased Public-Private collaboration

Post incident

- **Class actions** in Australia
- **Regulatory action** higher risk than **litigation from data subjects** affected the incident
- **Right of private action** exists in countries but not commonly used – yet
- **Liability of C-suite** – no cases but a developments in the US point to potential for personal liability of D&O

Post incident - claims management

Europe

- Principle costs: business interruption and system recovery and root cause analysis
- Third party claims:
  - incident ≠ "data breach"
  - "data breach" ≠ breach of legal obligations
  - But is certainly could be!
- Common procedural (expert) wisdom:
  - Claimant must set out and prove the (factual) requirements of the asserted claim
  - Relevant factual circumstances of an incident frequently 'hidden' in defendant's sphere
  - Exceptions can apply:
    - operational disruption may serve as indication for insufficient business continuity measures

Spot on the ECJ – C-340/21 (14 December 2023)

- VB ./. Bulgarian National Revenue Agency
  - Processing of various tax, social security data – millions of data subjects
- Confirmation of conventional GDPR wisdom: "data breach ≠ breach of legal obligations"!
- BUT: insufficient technical / organisational measures = breach of Art. 32 GDPR
  - Up to lower court to decide on a case-by-case basis
- AND: worries, anxieties and fears due to possible future misuse of the data could constitute non-material damage
  - Application – again – up to lower courts

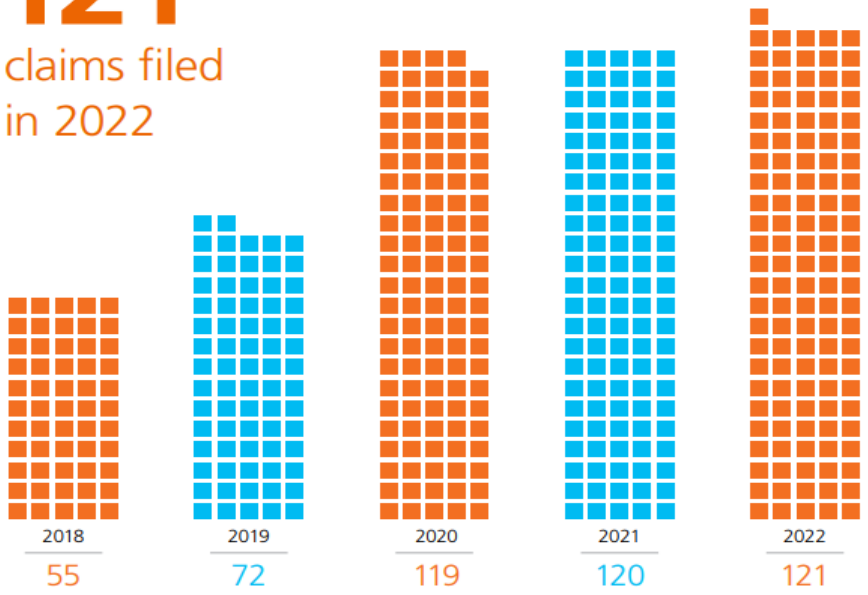
Post Incident - mass actions on the rise

Europe

Overall number of class actions

Europe and the UK continue to see record numbers of class actions being filed. Every year we have analysed has shown a consecutive increase.

121
claims filed
in 2022



With the Representative Actions Directive now being implemented across the EU, we anticipate yet further increases in the years to come.

Representative actions directive

Europe

- Came into force in December 2020
- Requires MSs to have “minimum procedural standards” for collective redress for consumer claims
- Opt-in device must be available; MSs can permit opt-out device
- Claims will be brought by Qualified Entities
- Categories of available claims include:
  - Unfair terms in consumer contracts (93/13/EEC)
  - Product liability directive (85/374/EEC)
  - GDPR (2016/679)
- MSs have 24 months to adjust domestic law; then 6 months to bring into force

Mass actions in the EU after Brexit

- Professional claim industry (experienced lawyers, experienced and sophisticated funders)
- The NL is a hub for claimants (European foundation of claim funders, branch offices of US plaintiff firms, etc)
- Mass actions increase across Europe (see our European Class Action Report)
- GDPR must be in scope of the mass actions according to the Rep Actions Directive
- In international incident multiple class or group actions simultanuously in various jurisdictions
- A number of mass actions are pending in the NL

Mass actions in the EU after Brexit - trending issues

Europe

- Each jurisdiction has its own issues (experienced courts, resources, language)
- Corporate governance of the claim vehicle
- Conflict of interest between funders and claimants
- Disclosure of funding mechanism/ review by the court?
- Cross border approach by claimants (combination of UK/Germany/NL/ Ireland claims)
- Combination of claims against Company, D&O, Accountants, Regulator (even POSI) to create a large potential pot of money)
- Specific GDPR issues:
  - Can individual claims for compensation of immaterial damage be aggregated?
  - Jurisdiction of the national court with a mixture of claimants and foreign defendants ?

Mass actions in the EU after Brexit - litigation funding

Europe

- Each jurisdiction has its own rules (No cure no pay, pars quota litis, anything goes)
- Sophisticated funders with expert counsel (both legal and financial)
- Conflict of interest between funders and claimants:
  - Who is in charge of the litigation strategy, funders or claimants?
  - Likewise, with settlement discussions
- Disclosure of funding mechanism/ review by the court?

4 Questions

Upcoming webinars

Product liability
Wednesday 5 June, 11.00 CET/10.00 UK

Litigation trends
Tuesday 9 July, 11.00 CET/12:00 UK

Main trends and traps when handling professional indemnity claims (European and not European jurisdictions)
Wednesday 11 September, 11.00 CET/12:00 UK

Claims handling
Wednesday 6 November, 10.00 CET/09:00 UK

Register now for our upcoming webinars

Click here or scan the QR code:

Thank you!

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

The information held in this publication is for general purposes and guidance only and does not purport to constitute legal or professional advice. It was prepared in co-operation with local attorneys.

CMS Legal Services EEIG (CMS EEIG) is a European Economic Interest Grouping that coordinates an organisation of independent law firms. CMS EEIG provides no client services. Such services are solely provided by CMS EEIG's member firms in their respective jurisdictions. CMS EEIG and each of its member firms are separate and legally distinct entities, and no such entity has any authority to bind any other. CMS EEIG and each member firm are liable only for their own acts or omissions and not those of each other. The brand name "CMS" and the term "firm" are used to refer to some or all of the member firms or their offices; details can be found under "legal information" in the footer of cms.law.

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