Waratah

ANALYTICS

No One Likes To Be Excluded

The Panel

• Éireann Leverett	- Panel Chair
• Sheila Wristberg	- iRisk management/reinsurance brokers Ghana
• Dixon Dela Aborjoe	- GCB Bank Ghana
• Otto Lee	- Hong Kong CERT
• Baiba Kaskina	- CERT.lv Latvia
• Cristine Hoepers	- CERT.br Brazil
• Rick Welsh	- Waratah

Poll

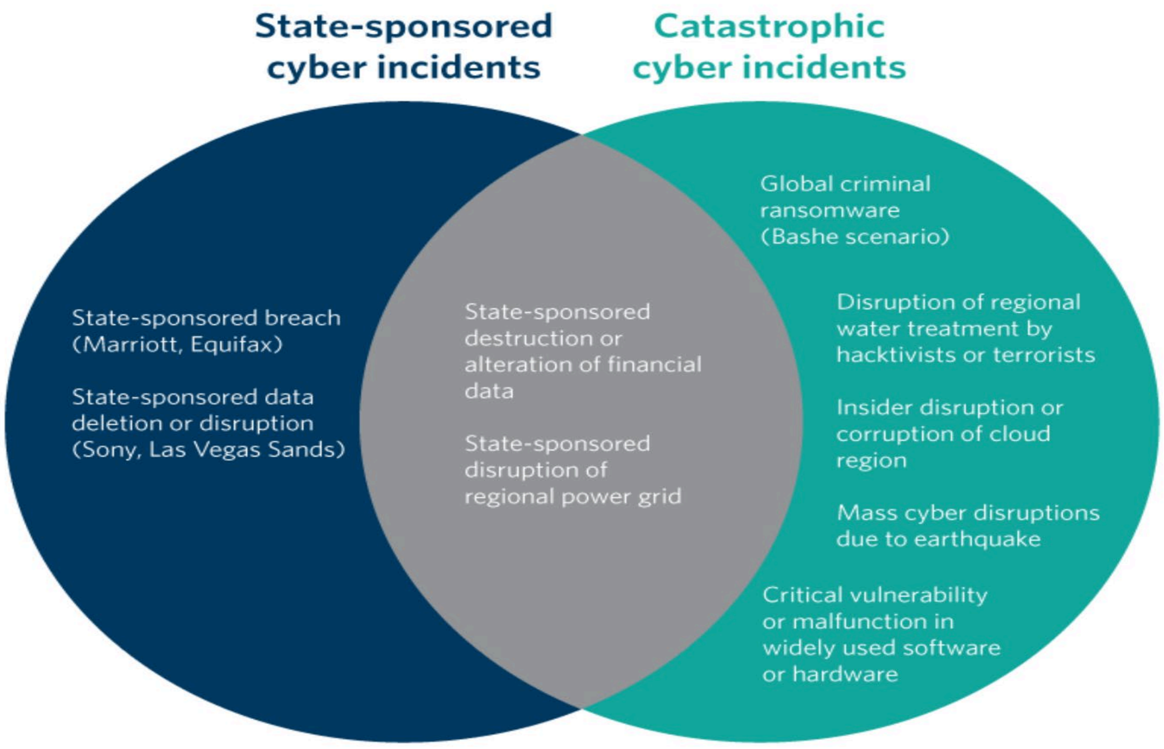
Have you ever been part of an incident where a cyber insurance claim was made?

Evolution of Traditional War Exclusions

- War exclusions have existed since the 1700s. Lloyd’s of London evolved exclusionary language from Spanish Civil War to London Blitz of WW2
- War is a correlated catastrophic, ongoing clash event. Highly destructive, potentially far-reaching in its geographic scope
- War therefore poses aggregation risks that are difficult for insurers to manage and cannot be predicted using actuarial analysis
- Insurance companies therefore came to exclude certain war-related claims to protect overall financial viability
- Insurers’ financial resilience comes from observing a combination of prudent capital requirements, proper reserving methods and adequate pricing.
- Regulators insist on insurance companies having sufficient capital to cover any reasonably foreseeable circumstances, and by making sure that the premiums they charge are adequate; if they aren’t then the regulator will require the insurance company to hold sufficient reserves to make up for any potential inadequacy.
- War presents incalculable systemic and catastrophic risk, an inability to underwrite, that is the inability to assess the probability of a war occurring, and the inability to estimate the scale of the damage if it did

Catastrophe Risk vs “State Sponsored”: What is CyberWar?

Imperfect Correlation Between State Sponsorship and Catastrophic Cyber Risk



State-sponsored cyber incidents

Catastrophic cyber incidents

State-sponsored breach (Marriott, Equifax)

State-sponsored data deletion or disruption (Sony, Las Vegas Sands)

State-sponsored destruction or alteration of financial data

State-sponsored disruption of regional power grid

Global criminal ransomware (Bashe scenario)

Disruption of regional water treatment by hacktivists or terrorists

Insider disruption or corruption of cloud region

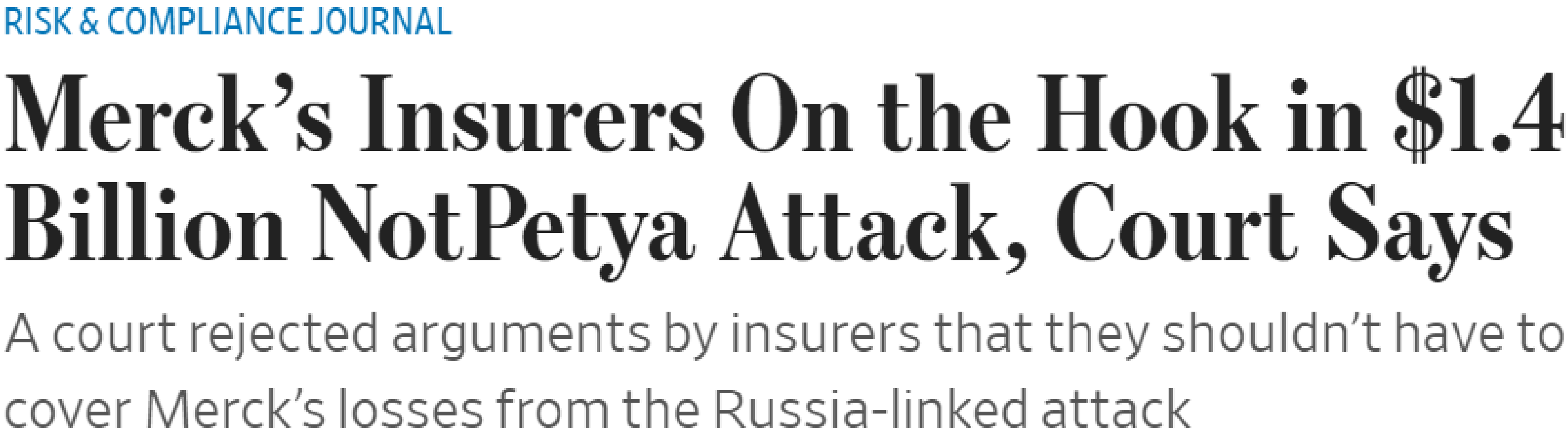
Mass cyber disruptions due to earthquake

Critical vulnerability or malfunction in widely used software or hardware

The 1.4 Billion Dollar Question

The cyber exclusions we are talking about today are the outcome of a long dialogue internal to the cyber insurance industry on ‘silent cyber’. The example below is **NOT FROM A CYBER INSURANCE POLICY,** illustrating what can go wrong for insurers when they are ‘silent on cyber’ in their all risks policies.

Hence the industry began work on exclusions clauses to get move towards a world with specific cyber insurance policies and other policies excluding it.

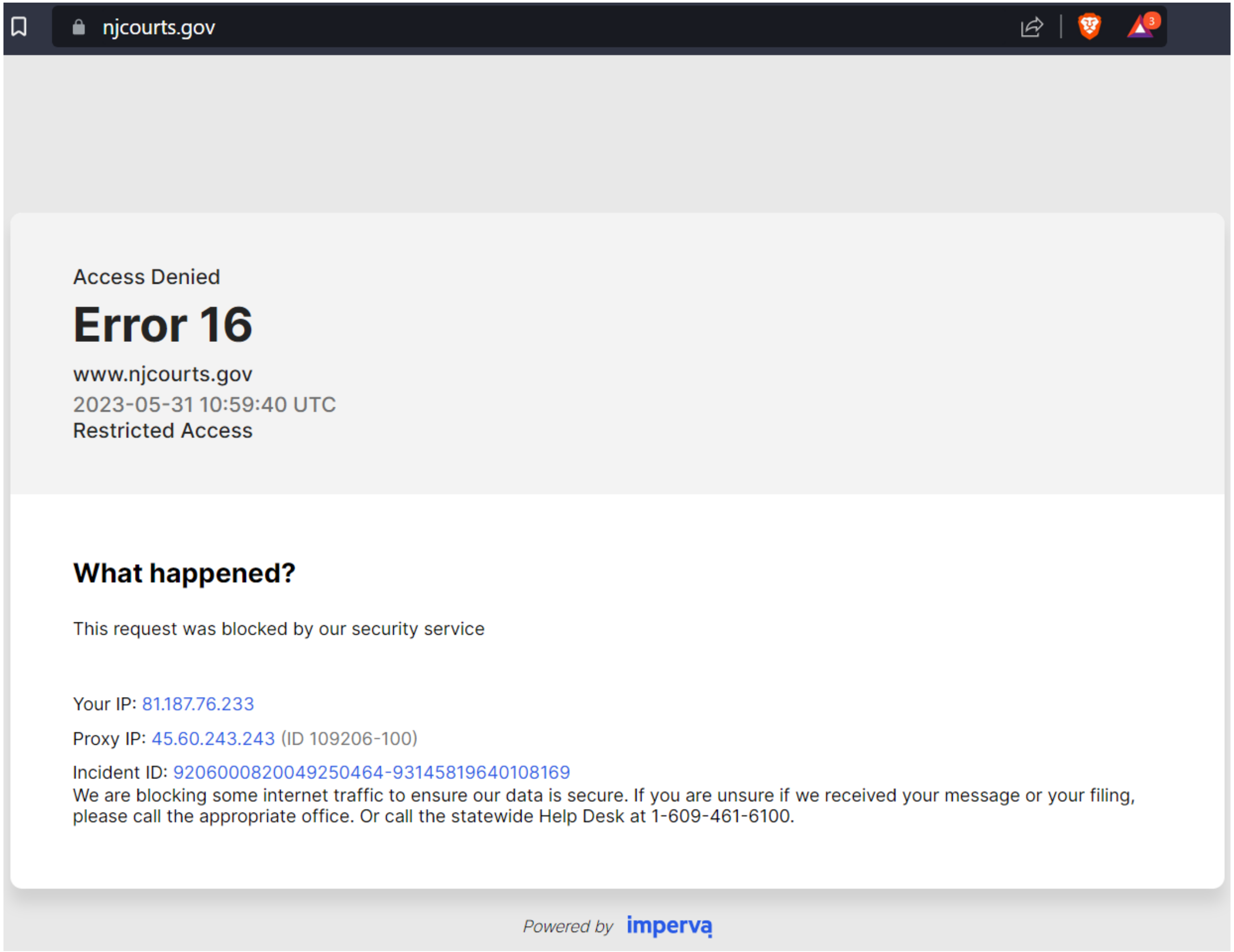


RISK & COMPLIANCE JOURNAL

Merck’s Insurers On the Hook in $1.4 Billion NotPetya Attack, Court Says

A court rejected arguments by insurers that they shouldn’t have to cover Merck’s losses from the Russia-linked attack

I wanted to give you the raw docket, but it seems they were down that day.



Access Denied

Error 16

www.njcourts.gov

2023-05-31 10:59:40 UTC

Restricted Access

What happened?

This request was blocked by our security service

Your IP: 81.187.76.233

Proxy IP: 45.60.243.243 (ID 109206-100)

Incident ID: 920600082004925046 4-93145819640108169
We are blocking some internet traffic to ensure our data is secure. If you are unsure if we received your message or your filing, please call the appropriate office. Or call the statewide Help Desk at 1-609-461-6100.

Poll

Have you heard of or read Lloyd’s Market Association's Cyber Exclusions?

The Exclusions: LMA5564A

Notwithstanding any provision to the contrary in this insurance, this insurance does not cover that part of any loss, damage, liability, cost or expense of any kind:

1.1. directly or indirectly arising from a war, and/or

1.2. **arising from a cyber operation. Attribution of a cyber operation to a state**

2. Notwithstanding the insurer’s burden of proof, which shall remain unchanged by this clause, in determining attribution of a cyber operation to a state, the insured and insurer will consider such objectively reasonable evidence that is available to them. **This may include formal or official attribution by the government of the state in which the computer system affected by the cyber operation is physically located** to another state or those acting at its direction or under its control. Definitions

…

4. Cyber operation means the use of a computer system by, at the direction of, or under the control of a state to:

4.1. disrupt, deny access to or, degrade functionality of a computer system, and/or

4.2. copy, remove, manipulate deny access to or, destroy information in a computer system.

…

5. State means sovereign state.

The Exclusions: LMA5565A

Largely the same but with limits on the amount instead of outright exclusion.

Subject to the exclusions above and the other terms, conditions and exclusions contained in this insurance, the following limits shall apply to any other **cyber operation(s)**:

2.1. *{response}* for any cover in relation to all loss arising out of one **cyber operation**;
2.2. *{response}* in the aggregate for the period of insurance.

These limits shall apply within the full policy limit and not in addition thereto.

The Exclusions: LMA5566A

“arising from a **cyber operation** that causes a **state** to become an **impacted state**. “

Introduces the idea of an impacted state where essential services were targeted.

“Essential service, means a service that is essential for the maintenance of vital functions of a **state** including but not limited to, financial institutions and associated financial market infrastructure, health services or utility services.

6. **Impacted state** means any **state** where a **cyber operation** has a major detrimental impact on:

6.1. the functioning of that **state** due to disruption to the availability, integrity or delivery of an **essential service** in that **state,** and/or
6.2. the security or defence of that **state**. “

The Exclusions: LMA5567A

Explores the differences of geographic location of computer and impacted state.

“1.3. arising from a **cyber operation** that causes a **state** to become an **impacted state.**

Paragraph 1.3 shall not apply to the direct or indirect effect of a **cyber operation** on a **computer system** used by the insured or its third party service providers that is not physically located in an **impacted state** but is affected by a **cyber operation**.”

The Exclusions: The B variants

These mostly cover different methods and means for making attributions.

“The sole difference between the ‘A’ and ‘B’ versions is that the latter do not contain agreement as to how a cyber operation is attributed to a state in order to determine whether the exclusion operates. Please note that Market Bulletin Y5381 states, amongst other requirements, that attribution be dealt with in the exclusion clause itself. Lloyd’s does however state in its bulletin that alternative approaches will be considered and where the requirements listed in the bulletin are not met, they will be considered on a case by case basis. Lloyd’s has also confirmed to the LMA that clauses which do not reference attribution will be considered by them so long as there is a mechanism for dealing with resolving questions of attribution in the policy or a robust reason can be given for why it is not required. If you wish to use any of the ‘B’ versions, you will need to evidence to Lloyd’s that a mechanism for addressing attribution has been agreed with insureds (or otherwise explain why it is not required). ”

Mondelez/Zurich

Provided coverage for “physical loss or damage to electronic data, programs, or software, including physical loss or damage caused by the malicious introduction of a machine code or instruction . . “ and “Actual Loss Sustained and EXTRA EXPENSE incurred by the Insured during the period of interruption directly resulting from the failure of the Insured’s electronic data . . .”

Mondelez/Zurich Exclusions 3.B.2.a. and 3.B.2.f.

[t]his Policy excludes loss or damage directly or indirectly caused by or resulting from:

a.) hostile or warlike action in time of peace or war, including action in hindering, combating or defending against an actual, impending or expected attack by any:

(i) government or sovereign power (de jure or de facto);

(ii) military, naval or air force; or

(iii) agent or authority of any party specified in I or ii above.

* * *

Poll

Do you believe the cyber war exclusions might have a chilling effect on your organisation's willingness to make attributions?

Poll

Do you think FIRST should advocate on cyber insurance policy where it impacts CERTs and DF/IR?

Questions?

Speaker Backgrounds

Cristine Hoepers
CERT.BR
NIC.BR

Cristine is the General Manager of CERT.br, the Brazilian National CERT of last resort, maintained by NIC.br, where she works since 1999.

In the past she served as a member of the FIRST Board of Directors, as a Lead Expert of the United Nations IGF Best Practices Forums on CERTs and on Spam, and as a member of the ITU High Level Experts Group on Cybersecurity. In 2020 she received from M3AAWG the annual Mary Litynski Award for her work to reduce Internet abuse and increase Internet resilience.

She holds a Ph.D. in Applied Computing from the Brazilian National Institute for Space Research.

Baiba Kaškina
CERT.**LV**

Baiba is the General Manager of CERT.LV - Latvian National and Governmental CSIRT (since 2011) leading the dynamic work of the team and liaising with the constituencies. She has started the first CERT team in Latvia in 2006 and since then has been involved in shaping the cyber security ecosystem of Latvia as well as internationally.

Baiba has been the chair of European CSIRTs collaboration forum TF-CSIRT from 2014-2019 and is the Chair of the FIRST Membership Committee since 2022.

She has received the Order of Three stars from the Republic of Latvia in recognition of her contribution to establish and lead the Latvian cyber security environment.

Speaker Backgrounds

Sheila Wristberg
iRisk Partners

Sheila is an insurance broker and risk management consultant with over a decade of experience in providing professional services to clients. She is the Managing Director of iRisk Management Limited and Director of iRisk Reinsurance Brokers. She has grown the iRisk brand to become the number 5 insurance brokerage firm in Ghana, out of a 120-firm market.

She is a Chartered Accountant, former Big Four auditor and tax consultant, and has advised on multi-million-dollar agreements and projects throughout Africa. Her expertise lies in risk structuring and advisory services for high-level government projects and developing insurance solutions for SMEs and underdeveloped markets. Sheila is an executive council member of the Insurance Brokers Association of Ghana (IBAG) and serves as their Vice-Treasurer. In 2022, the African Insurance Organisation (AIO) and Young Insurance Professionals (YIPs) named her first runner-up for the Maiden Excellence Awards for young insurance professionals in Africa.

She was also named Angaza Awards Top 10 African Women to Watch in Banking, Finance & Investment and WIMATop 50 Awards by Women Leaders in Management Africa (WIMA) in 2023. She is the founder of Women Leadership in Insurance Africa, which is a leadership development network for female professionals working in insurance, risk management, sustainability and ESG in Africa and the diaspora.

Dixon D Aborjoe
GCB Bank

I am a cyber security practitioner with 12 years' experience within the banking financial sector in Ghana and the African continent dealing with cyber security incident responses at the various level. Current The representative of FIRST for GCB Bank PLC SOC and the manager for GCB BANK PLC Security Operations ad incidence. Also a certified ISO/IEC 27032 Senior Lead incident Manager.

Speaker Backgrounds

Rick Welsh
Waratah

- Rick has 20+ years experience underwriting Cyber insurance and established the first dedicated Cyber insurance practice at Lloyd's in 2000 which has now grown to be the market's largest Cyber insurance platform globally.
- Contributed to Lloyd's cyber knowledge base through RDS scenario development and many conference and market forums

Eireann Leverett
Concinnity Risks

- Eireann is ranked in the Top ten of google scholar Cyber Risk and Cyber Insurance researchers and was part of the multidisciplinary team that built the first cyber risk models for insurance with Cambridge University Centre for Risk Studies and RMS.
- He is the (co)author of "Solving Cyber Risk" and numerous papers on the aggregation of cyber security risk, lead contributor to Lloyds' RDS research paper "Business Blackout"

Otto Lee
HKCERT

- Otto has over 20 years of experience in information security and cybersecurity, specializing in cloud security, data protection and privacy, and incident response. He has worked extensively in the financial services industry, and serving as an Asia representative to handle security incidents from APAC countries. He holds certifications including CCSP, CISSP, CSSLP, CISA, CDPSE and GLEG.
- Otto is Head of HKCERT. Previously, he was Security Assurance Lead for AWS's New Markets in APAC, engaging with regulators on data privacy for Hong Kong and beyond.

References

1. https://www.lmalloyds.com/LMA/News/LMA_bulletins/LMA_Bulletins/LMA21-042-PD.aspx
2. https://www.lmalloyds.com/LMA/News/LMA_bulletins/LMA_Bulletins/LMA23-002-PD.aspx
3. https://www.njcourts.gov/system/files/court-opinions/2023/a1879-21a1882-21.pdf