Prof. Dr. Robert Koch LL.M. (McGill)
Managing Director of the Institute of Insurance Law (est. 1916)

Coverage for Ransomeware Attacks in Germany

XVI AIDA World Congress

30 September 2023

Working Party: Financial Lines and Cyber

University of Hamburg

Faculty of Law

Overview

I. Introduction

II. Increase in ransomware attacks

III. Insurer and government response to increasing ransomware attacks

IV. Guidelines on the provision of ransom insurance issued by the German Federal Financial Supervisory Authority's (Bafin)

V. Coverage for cyber extortion loss

VI. Cover for cyber extortion loss as mitigation costs

VII. Conclusion

II. Increase in ransomware attacks

Dimension of the Damage and Profit		
Ø-Ransom 2021: 204.695 US-Dollar	Annual damage from ransomware	Profit through ransomware groupings 2021:
Ø-Ransom 2020: 169.446 US-Dollar	2021: ca. 24,3 Bill. Euro.	602 Mill. US-Dollar
Increase by 21%	2019: ca. 5,3 Bill.. Euro	

Source: Bundeskriminalamt (German Federal Criminal Police Office)

III. Insurer and government response to increasing ransomware attacks

- Insurance Industry
  - no more coverage for ransomware under cyber insurance (AXA and Generali in France)
  - in the German market, no exclusions, but sublimits for insurance of ransom payments (as a main benefit)
- Government
  - Conference of Federal State Interior Ministers in 2021:
    - it is to be examined whether ransom payments should be excluded from insurance coverage
  - German Federal Government in 2022:
    - ban on ransomware insurance would interfere with the constitution and
    - would not prevent companies from paying ransoms themselves

IV. Guidelines on the provision of ransom insurance issued by the German Federal Financial Supervisory Authority's (Bafin) in 1998 (1)

"Providing this type of insurance in compliance with public policy is, …, only possible if account is taken of the fact that these particularly sensitive contracts require a high degree of confidentiality and must not hinder the investigative work of the police. Furthermore, collusive cooperation between perpetrators, victims, or insurance personnel must be avoided."

IV. Guidelines on the provision of ransom insurance issued by the German Federal Financial Supervisory Authority's (Bafin) in 1998 (2)

Ransom insurance in cyber policies is permitted under certain conditions, i.e.

- advice by a security consultant based on a security concept
- non disclosure of the ransom insurance cover by the policyholder
- sum insured must correspond to the economic situation of the company in order to avoid an increase in subjective risk
- sole responsibility of a department for administration and claims handling that reports directly to the policyholder's management board
- obligation of the policyholder and the insurer to immediately report the extortion to the police and to cooperate with the law enforcement authorities

https://www.bafin.de/dok/10023564 and
https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Rundschreiben/rs_9803_va_loesegeldversicherung_en.html

V. Coverage for cyber extortion loss (1)

V. Coverage for cyber extortion loss (2)

Cyber extortion clause

I.4.1. CYBER EXTORTION

The Insurer shall provide cover for Cyber Extortion Loss incurred by the Insured Companies due to Cyber Extortion. This coverage is subject to a Sub-limit as specified in the schedule

VII.9. CYBER EXTORTION LOSS

Cyber Extortion Loss means

a) the necessary reasonable fees and expenses and costs, for external experts that are incurred by the Insureds, following prior written consent of the Insurer, in direct relation to the assessment and response to an incident of Cyber Extortion;

b) b) amounts of money paid by the Insureds, following prior written consent by the Insurer, for the purpose of defending against or putting an end to an incident of Cyber Extortion (ransom and/or blackmail payments). Payment using a crypto-currency, such as BitCoins, shall also be deemed payment of an amount of money.

VI. Cover for cyber extortion loss as mitigation costs (1)

In addition to sub-limited cover or in case of no cover for cyber extortion loss if payment prevents business interruption?

- Under German Insurance law (VVG), insurer must indemnify the insureds for the expenses incurred in averting or mitigating the insured loss up to the sum insured for the loss that the insured (attempted) to avert or mitigate, § 83 para. 1 and 3 VVG (mandatory provision)
  - Payment of a ransom for a stolen car insured as mitiga-tion costs in comprehensive car insurance (Court of Appeal Saarbrücken, NJW-RR 1998, 463; District Court Freiburg, zfs 2001, 174).
  - Ransom paid to pirates to recover the ship and cargo is insured as mitigation costs in marine insurance (no case law, only scholarly writings).

IV. Cover for cyber extortion loss as mitigation costs (2)

§ 83 VVG Reimbursement of expenses

(1) [1]The insurer shall reimburse expenses incurred by the policyholder [to avert or mitigate the loss], even if they have been unsuccessful, to the extent that the policyholder was entitled to consider them necessary under the circumstances…

(2) …

(3) Expenses incurred by the policyholder in accordance with the insurer's instructions shall also be reimbursed to the extent that, together with the other indemnification, they exceed the sum insured.

IV. Cover for cyber extortion loss as mitigation costs (3)

§ 83 VVG Reimbursement of expenses

(1) [1]The insurer shall reimburse expenses incurred by the policyholder [to avert or mitigate the loss], even if they have been unsuccessful, to the extent that the policyholder was entitled to consider them necessary under the circumstances…

→ Prerequisite "consider necessary under the circum-stances" irrelevant if measure objectively necessary" i.e.

ransom sum < cover for business interruption

IV. Cover for cyber extortion loss as mitigation costs (4)

How Long Does It Take to Recover from a Ransomware Attack:

https://www.provendata.com/blog/how-long-does-it-take-to-recover-from-ransomware/:

"According to a Statista survey, the average recovery time after a ransomware attack is 22 days…

Example:

ransom sum: 1 Mill. Euro

Insured daily compensation rate: 200.000 Euro

→ payment is objectively necessary under the circumstances

→ if insured pays the ransom it is entitled to reimbursement

IV. Cover for cyber extortion loss as mitigation costs (5)

I.5.1. CYBER-CRISIS MANAGEMENT

The Insurer shall cover the reasonable fees and expenses incurred in relation to an external cybercrisis manager… subject to the prior written consent of the Insurer…, due to… Cyber Extortion in order to receive advice with regard to the strategic management of a cyber crisis for the purpose of adverting or minimizing loss or damage…

I.5.7. RESCUE COSTS (Allianz Cyber Protect Premium)

The Insurer shall provide cover for expenses incurred by an Insured Company, following prior written consent of the Insurer,

a) which, given the circumstances, are necessary to avert the imminent assertion of a Claim insured under this policy and

b) which do not exceed the amount of said Claim.

IV. Cover for cyber extortion loss as mitigation costs (6)

§ 82 VVG Averting and mitigating the damage

(1) Upon occurrence of the insured event, the policyholder shall take all possible steps to avert and mitigate the loss.

(2) [1]The policyholder must follow the insurer's instructions as far as is reasonable for him and must obtain instructions if circumstances permit...

→ No obligation to follow the insurer's instructions if the instructions impose an unreasonable financial burden on the policyholder

Example:

Insured daily compensation rate: 200.000 Euro/provided for 20 days (max. 4 Mill. Euro), ransomware attacker demands 2 Mill. Euro.

10 days after the attack, it becomes clear that the insured needs more than 20 days to resume business operations (i.e., the damage caused by the business interruption exceeds the sum insured). The insured is allowed to pay 2 mill. euros to the extortionist without the insurer's consent and is entitled to this sum as mitigation costs.

V. Conclusion

Under current German insurance law,

- regardless of an agreed sublimit for cyber extortion
- cyber insurer always owes ransom payment up to the sum insured for business interruption
- as expenses for mitigating the loss
- if the ransom sum is less than the actual/anticipated business interruption loss and/or the costs of restoring the data

Thank you for your attention!

robert.koch@uni-hamburg.de