UNIVERSITÄT
HEIDELBERG
ZUKUNFT
SEIT 1386

Cyber Risks as a Challenge for Corporations and their Executives in Germany
(Duties, Liability)

Frankfurt, 23 March 2023

Dirk Verse
Heidelberg University

LockBit Black Ransomware

Your data are stolen and encrypted

The data will be published on TOR website

[redacted]

and [redacted] if you do not pay the ransom

You can contact us and decrypt one file for free on these TOR sites

http://[redacted]

http://[redacted]

Decryption ID: 3[redacted]

Royal Mail ransomware attackers threaten to publish stolen data

The Guardian

Postal service has been unable to send letters and parcels overseas since Wednesday due to hacking

Thu 12 Jan 2023 22.24 GMT

Royal Mail has been hit by a ransomware attack by a criminal group, which has threatened to publish the stolen information online.

The postal service has received a ransom note purporting to be from LockBit, a hacker group widely thought to have close links to Russia.

CYBERCRIME

Ransomware Gang Offers to Sell Files Stolen From Continental for $50 Million

A notorious ransomware group is offering to sell files allegedly stolen from German car parts giant Continental for $50 million.

By Eduard Kovacs
November 10, 2022

A notorious ransomware group is offering to sell files allegedly stolen from German car parts giant Continental for $50 million.

Continental reported in August that it had been targeted in a cyberattack that resulted in hackers accessing some of its systems. The company said at the time that the attack had been "averted" and that business activities were not affected.

UNIVERSITÄT HEIDELBERG
ZUKUNFT SEIT 1386

I. Some facts on cyber risks

Cyber attacks as a prime business risk

- Estimated damage for the German economy > EUR 200 billion p.a. (BITKOM Research 2022)
- 45% of the German businesses (with ≥ 10 employees) regard cyber attacks as an *existential* risk to their business, 78% of them expect the number of cyber attacks to further increase (BITKOM Research 2022)
- Alongside supply chain disruption, cyber incidents are regarded *the* top business risk by risk managers in Germany and Europe (Allianz Risk Barometer 2023)
- BSI (German Cybersecurity Authority) Report 2022: *"The threat in cyberspace is higher than ever."*
  - Ukrainian-Russian war as an aggravating factor

UNIVERSITÄT HEIDELBERG
ZUKUNFT SEIT 1386

I. Some facts on cyber risks

Ransomware attacks in particular

- Cyber attacks occur in numerous forms and for numerous purposes, but ransomware is currently the “main threat” (BSI report 2022)
  - BSI observes that the attacks are becoming more and more professional
  - “Ransomware as a service” as an additional driver
- Russia is suspected to be the main country of origin of ransomware attacks
  - It is estimated that more than 70% of ransomware revenue in 2021 went to recipients affiliated with Russia in some way (Chainalysis 2022)
- While the authorities recommend not to pay the ransom, many victims still pay
  - > 40% in Germany in 2021 (Sophos 2022)
- Insurance coverage
  - Most mid-sized and large companies in Germany have insurance coverage for ransomware attacks (Sophos 2022); insurance cover may also extend to the payment of ransom fees

II. Legal framework for corporations

NIS 2 Directive: mandatory cybersecurity measures in critical sectors

- Directive (EU) 2022/2555 (“NIS 2”) to be implemented by 17 Oct. 2024
- NIS 2 provides duties for entities in certain defined critical sectors (“essential and important entities”, EIE):
  - Cybersecurity risk-management: EIE must take “appropriate and proportionate technical, operational and organizational measures” to prevent disturbances of their IT systems, “taking into account the state-of-the-art” (Art. 21)
  - Reporting: EIE must notify any significant incident within 24 hours, and file reports on the cause of the incident and the mitigation measures (Art. 23)
  - Competent authorities have far-reaching supervisory powers to monitor compliance; non-compliance triggers severe administrative fines (up to 2% of the group worldwide annual turnover for essential entities, Art. 34)

II. Legal framework for corporations

NIS 2 Directive: mandatory cybersecurity measures in critical sectors (2)

- Wide scope of application
  - NIS 2 extends the list of critical sectors
    - Sectors of high criticality (Annex 1): energy, transport, banking, financial market infrastructures, health, drinking water, waste water, digital infrastructure, ICT service management (b2b), public administration, space
    - Other critical sectors (Annex 2): postal services, waste management, production/ distribution of chemicals, production/distribution of food, manufacturing (esp. medical devices, electronic products, machinery, motor-vehicles), digital providers, research
  - NIS 2 includes all companies in the critical sectors except small companies (< 50 employees or < 10 million EUR turnover), no additional materiality threshold (!)

→ Large parts of the industry are covered by NIS 2

- Currently, roughly 450 critical infrastructures in Germany are subject to mandatory cybersecurity and reporting obligations (under the German IT Security Act [BSIG]).
- By contrast, an estimated 40,000 entities (!) in Germany will fall under NIS 2.

UNIVERSITÄT HEIDELBERG
ZUKUNFT SEIT 1386

II. Legal framework for corporations

NIS 2 Directive: mandatory cybersecurity measures in critical sectors (3)

- Which cybersecurity risk-management measures are required?

  The measures shall include at least the following (Art. 21 [2] NIS 2):

  (a) policies on risk analysis and information system security;

  (b) incident handling;

  (c) business continuity, such as backup management and disaster recovery, and crisis management;

  (d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;

  (e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;

  (f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures;

  (g) basic cyber hygiene practices and cybersecurity training;

  (h) policies and procedures regarding the use of cryptography and, where appropriate, encryption;

  (i) human resources security, access control policies and asset management;

  (j) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

II. Legal framework for corporations

DORA: sector-specific regulation for financial institutions

- Digital Operational Resilience Act ("DORA", Regulation [EU] 2022/2554) provides cybersecurity risk management and reporting requirements for financial institutions
  - "lex specialis" in relation to NIS 2 (recit. 16)
  - DORA will apply from 17 Jan. 2025, supersedes current regulation in the Member States (in Germany § 25a KWG, § 26 VAG in conjunction with BaFin circulars BAIT and VAIT)
- DORA risk-management requirements are (much) more detailed than the NIS 2 rules
  - Example: Art. 6 (4) DORA provides that the IT control function in financial institutions should be sufficiently independent and separated in order to avoid conflicts of interest,

II. Legal framework for corporations

Further legislation on cybersecurity

- Data Protection: General Data Protection Regulation ([EU] 2016/ 679, “GDPR”)
  - Controllers and processors of personal data *“shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk”* (Art. 32).
  - In case of a personal data breach (data leak), the breach must be notified to the competent authority (Art. 33) and in certain circumstances also to the persons affected (Art. 34).
  - Non-compliance can trigger severe fines (Art. 83 [4]) and civil liability (Art. 82).
- [Product-related legislation
  - Cybersecurity Act (Regulation [EU] 2019/881): EU framework for the certification of IT products and services
  - Draft Cyber Resilience Act (COM [2022] 454): Commission proposal to introduce cybersecurity requirements for products with digital elements]

II. Legal framework for corporations

Dealing with ransom demands in particular

- Dealing with ransom demands
  - No special legislation in the EU/Germany
  - The majority view is that ransom payments are, at least as a general rule, not illegal under German law (though some argue it could be illegal support of a criminal association).
  - German authorities recommend not to pay (not binding)
- Ban on ransom insurance?
  - Currently, there is a debate in Germany whether insurance cover for ransom payments should be prohibited.
  - So far, ransom insurance is permissible subject to certain restrictions (no advertisement for ransom insurance, insurance cover must be kept confidential, incident must be reported to the police).
  - The critics argue that ransom insurance fosters the readiness to pay ransoms and thus fuels the development of the ransomware industry.

III. Directors‘ duties and liability

Overview of directors’ duties

- General duty of care, § 93 (1) Stock Corporation Act (AktG), § 43 (1) Act on Limited Liability Companies (GmbHG)
  - Duty of legality: directors must take all necessary and reasonable precautions that the company complies with applicable law (NIS 2 implementing legislation, DORA, GDPR etc.).
  - Duty to act in the best interest of the company
    - Where a company is not subject to mandatory legal cybersecurity requirements, the directors are still bound to prevent harm from the company by taking precautions against cyber risks in the own interest of the company.
    - In this case, the decision to what extent investments in cybersecurity serve the corporate interest is a business decision, *i.e.* the BJR applies (§ 93 [1] s. 2 Stock Corporation Act).

UNIVERSITÄT HEIDELBERG
ZUKUNFT SEIT 1386

III. Directors‘ duties and liability

Decisions to be taken at board level

- To what extent can the directors delegate cybersecurity risk-management tasks to employees?
  - Prevailing view: the management board (MB) members must not delegate the fundamental entrepreneurial decisions (“Leitung”, § 76 AktG)
  - Given the outstanding importance of cyber risks, it is widely accepted that the cybersecurity strategy is a “matter for the boss” (“Chefsache”)

    → MB must decide on a cybersecurity strategy that contains at least the guiding principles and the basic structure of the company’s cybersecurity organization

    (incl. adequate resources for prevention and response measures, clear roles and responsibilities, reporting lines, regular reviews of the system etc.).
  - The fact that cybersecurity is a “matter for the boss” is now also emphasized in NIS 2 and DORA (see below).

UNIVERSITÄT HEIDELBERG
ZUKUNFT SEIT 1386

III. Directors‘ duties and liability

Decisions to be taken at board level (2)

- Art. 20 NIS 2 (for essential and important entities in critical sectors):

  (1) Member States shall ensure that the management bodies of essential and important entities approve the cybersecurity risk-management measures taken by those entities in order to comply with Article 21 [cybersecurity risk-management], oversee its implementation and can be held liable for infringements by the entities of that Article…

  (2) Member States shall ensure that the members of the management bodies of essential and important entities are required to follow training, and shall encourage essential and important entities to offer similar training to their employees on a regular basis…”

UNIVERSITÄT HEIDELBERG
ZUKUNFT SEIT 1386

III. Directors‘ duties and liability

Decisions to be taken at board level (3)

- Art. 5 DORA (for financial institutions):

“…the management body shall:

(a) bear the ultimate responsibility for managing the financial entity’s ICT risk;

(b) put in place policies that aim to ensure the maintenance of high standards of availability, authenticity, integrity and confidentiality, of data;

(c) set clear roles and responsibilities for all ICT-related functions (…);

(d) bear the overall responsibility for setting and approving the digital operational resilience strategy (…);

(e) approve, oversee and periodically review the implementation of the financial entity’s ICT business continuity policy and ICT response and recovery plans (…);

(f) approve and periodically review the financial entity’s ICT internal audit plans, ICT audits and material modifications to them;

(g) allocate and periodically review the appropriate budget to fulfil the financial entity’s digital operational resilience needs in respect of all types of resources, including relevant ICT security awareness programmes and digital operational resilience training (…) and ICT skills for all staff;

(h) approve and periodically review the financial entity’s policy on arrangements regarding the use of ICT services provided by ICT third-party service providers;

(i) put in place, at corporate level, reporting channels enabling it to be duly informed of the arrangements concluded with ICT third-party service providers on the use of ICT services (…).”

III. Directors‘ duties and liability

Directors’ liability

- Any negligent breach of a director’s duty that causes a damage to the company triggers liability towards the company, § 93 (2) AktG, § 43 (2) GmbHG.
  - According to the prevailing view, even in the case of only light negligence the directors are liable for the full amount of the damage even it is extremely high.
- Burden of proof
  - The company only has to prove that an act or omission of a director has caused a financial loss to the company.
  - It is then up to the director to prove that there was no breach of duty (BGHZ 152, 280).

  → If the company suffers a loss from a cyber incident, the directors must prove that the incident occurred although they had put in place appropriate prevention and response measures and fulfilled all their duties under applicable law (NIS 2, DORA, GDPR).
  - Cybersecurity certifications (e.g. compliance with ISO 27001 on IT security) may help to bring this proof, but they do not provide a safe harbor
- In conclusion, cyber risks pose a very significant risk not only for companies, but also for their directors. As a result, cyber insurance plays an ever-increasing role.

UNIVERSITÄT
HEIDELBERG
ZUKUNFT
SEIT 1386

Thank you!

Dirk A. Verse
Professor of Private Law and Business Law
Director of the Institute for German and European
Corporate and Economic Law
Heidelberg University
dirk.verse@igw.uni-heidelberg.de