



Munich Personal RePEc Archive

# **What do cyber- attacks and pandemics have in common? Some lessons from the German medical practices behaviour.**

Pitterle, Claudia

Doctoral School of Economics and Business Administration  
University Alexandru Ioan Cuza Iasi- Romania

2021

Online at <https://mpra.ub.uni-muenchen.de/117728/>  
MPRA Paper No. 117728, posted 05 Jul 2023 13:57 UTC

# What do cyber- attacks and pandemics have in common? Some lessons from the German medical practices behaviour.

CLAUDIA PITTERLE

Doctoral School of Economics and Business Administration  
University Alexandru Ioan Cuza Iasi- Romania

pitterle.c@gmail.com  
+49 178 814 814 8

---

**Abstract:** An independent IT security consultant<sup>1</sup> and one of Germany's best-known hackers compares the issue of cyber-attacks in Germany with the rise of the Covid 19 pandemic. Both risks are growing enormously fast, are very difficult to stop and cause very great damage. Possibilities of mitigation and treatment are provided by vaccines and intensive care beds as well as the elimination of vulnerabilities in the company and cyber insurance. However, there is often a lack of understanding of prevention and treatment.

A look at Germany shows the Hiscox Cyber Readiness Report 2021 (Hiscox, 2021). Out of 1030 companies surveyed in Germany in 2021, 46% said they had experienced a cyber-attack in the last 12 months. In 2020, this figure was still 41%.

Own conducted in-depth interviews with doctors in private practice in autumn 2020 have shown that the need for such insurances is non-existent.

It is very easy to take appropriate measures in Germany and there are many companies and service providers that offer their products for example a cyber insurance for this purpose. Nevertheless, many companies or doctors' practices decide against taking out an insurance, or do not deal with these existentially threatening issues. Possible explanations are provided by behavioural economics. In particular, judgement heuristics or "classical" heuristics such as representativity, availability and anchoring/adjustment show such explanations (Pfister et al. 2019 p.133 ff and Theil 2002 p.55 ff).

This study reports on the situation in German medical practices. In particular, doctors in private practice (self-employed) with employees. As a self-employed medical practitioner, one not only bears the responsibility for the patients, but also for one's own existence and the employees.

The current research is a report of an ongoing dissertation that deals, among other things, with the topic of cyber-attacks and the possibility of protecting a cyber insurance.

The research question emerged from the researcher's prior understanding and practical experience of over 20 years of client counseling.

***Index terms:* Cyber Attacks, Cyber Insurance, Doctor's practice, sales losses, judgment heuristics, behavioral economics**

---

## I. INTRODUCTION

Initial situation-a doctor<sup>2</sup> who runs his own surgery should act responsibly for himself and his employees and protect himself against economic damage. In the event of a loss of business, wages, rents, etc. must continue to be paid. Similarly, regulations must be made when a doctor, for example becomes ill, who then continues his surgery. In addition, there are constantly increasing numbers of cyber-attacks in Germany on patient data. Economic damage can be insured in Germany with existing insurances.

In recent years, cybercrime has also increased in Germany. Medical surgeries have become victims of blackmailers (GDV, 2019). Patient data has been stolen or blocked due to poorly secured servers. Doctors are blackmailed into paying ransoms. Medical surgeries stand still for days and the doctors have to bear not only the loss of reputation but also the loss of business. This risk is completely underestimated in German medical surgeries.

A survey by the German Insurance Association found, 44% of doctors see the risk of a cyber-attack on a doctor's office as very high. However, only 17% see themselves as the victim of an attack (GDV, 2019).

---

<sup>1</sup> <https://www.gdv.de/de/themen/positionen-magazin/kolumne--die-schwachen-zuerst-68232>

<sup>2</sup> The generic masculine is used for easier reading

In the case of a cyber-attack described above, 37.000EUR<sup>3</sup> can be quickly accumulated.

In group surgeries, the damage is multiplied by the number of doctors. In addition, there is a loss of reputation for the surgery, which is very difficult to quantify.

Using the example of a cyber-attack, the following illustrates what costs a doctor faces and what insurance covers. This example can be found in the industry report: Cyber risks of doctors and pharmacies (GDV, 2019). A cyber-attack often begins with the theft of patient data. The hackers demand a ransom by means of a blackmail letter. This is intended to prevent the publication of the data. The following costs are incurred: Information costs to patients of 4.000EUR, Involvement of a lawyer 2.000EUR, security assistance 5.000EUR, two days of business interruption 5.000EUR, claims for damages from patients due to published data according to Art. 82 DSGVO (liability and right to compensation) (DSVGO, 2018) 20.000EUR, crisis communication 1.000EUR. These costs of 37.000EUR can be covered by insurance.

Further costs are incurred that have not yet been taken into account, the doctor must report the attack to the State Data Protection Commissioner within 72 hours. The state data protection commissioner will then decide whether and how to inform the potentially affected patients. I.e. depending on the federal state, a registered letter with return receipt is required for this. Postage costs per letter are 5,50 euros. With only 4.000 patients' data, the costs amount to another 22.000EUR. These can also be covered by insurance.

During the one-hour depth interviews in autumn 2020, the five doctors were also asked about cyber risk insurance. None of the five doctors interviewed has such insurance or sees the need for such insurance cover. Arguments against this insurance included, "we have a software service provider who maintains the systems", "my practice is too insignificant", "the server only runs during the day", "we are sufficiently protected".

These answers are also reflected in the GDV surveys already mentioned. Here, 56% of the doctors surveyed emphasised that their practice is too small to come into the focus of cybercriminals. Likewise, 80% of the respondents think that the existing computer systems are sufficiently protected.

This is in line with the conducted depth interviews by the researcher in autumn 2020.

## II. METHOD

Richter et al. (2018) describe considerations from the perspective of modern behavioral economics on how

needs and decision processes of insurance customers can be better understood. Using a selection of behavioral patterns, judges illustrate how insurance is not contracted and risks are misperceived.

Pfister et al. (2019 p.133 ff) refers to the "classical" heuristics, representativity, availability and anchoring/adjustment. These are proposed by Tversky and Kahneman and are considered the most important heuristics. A heuristic is a simple rule - also called a rule of thumb - that simplifies the formation of judgements. Especially in complex problems, such as making decisions, a simple rule is used. "Heuristics often lead to correct or approximately correct judgments and decisions, but under certain conditions can systematically lead to misjudgments (bias)" Richter et al.2019 p.133.

.... people rely on a limited number of heuristics principles which reduce the complex tasks of assessing probabilities and predicting values to simpler judgmental operations. In general, these heuristics are quite useful, but sometimes they lead to severe and systematic errors (Tversky & Kahneman 1974, p. 1124).

The multitude of daily decisions can be facilitated by judgement heuristics, according to Theil M. (2002 p 55 ff). The application is mostly successful but can lead to systematic errors (Jungermann and Slovic p 188, see Bechmann, G.1993).

"Two areas are of particular importance here: the assessment of low-probability events is particularly prone to error, and the search for causal relationships ends as soon as a satisfactory solution has been found" (Theil M. 2002 p. 56).

For illustration purposes, the three heuristics are presented below and their relevance to insurance demand explained, see Theil M. 2002 p.55- 98 and Richter et al. 2018 p.8

**Representativeness-** this is about the extent to which an object, person, situation or condition is considered representative of a class. These characteristics influence frequencies and probability estimates. Thus, this heuristic is held responsible for biases in the estimation of probabilities and influences the assessment of the extent of damage. (Theil M. 2002 cited in Williams and Heinz 1971 p.66 f) "It won't happen to me" a damage event can thus not be considered representative. (Jungermann and Slovic p.189, see Bechmann, G.1993).

**Availability-** mental availability refers to the fact that some information is easier to imagine, remember and recall than others. This can lead to judgements about possibilities or probabilities being significantly

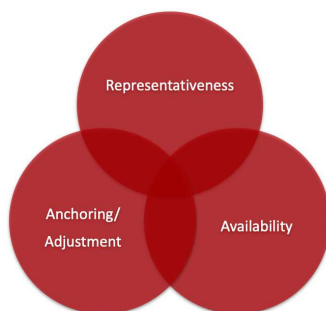
3

<https://www.gdv.de/resource/blob/48328/ae262d6702e2d9f>

5446c780a22450d23/download-branchenreport-cyber-aerzte-und-apotheker-data.pdf

influenced. (Theil M. 2002 cited in Slovic, Fischhoff and Lichtenstein (1977) p.4; Watson and Buede (1987) p.86; Einhorn and Hogarth (1971) p.67; Eisenführ and Weber (1999) p.367; Kittner (1994) p.80f). This availability heuristic is thus also seen as a suitable basis for assessing a risk, as certain events are easier to imagine (Theil M. 2002 cited in Slovic, Fischhoff and Lichtenstein (1981) p. 465). The insurable risks of an insurance policy often have low probabilities of occurrence, although the extent of the damage can be worrisome, and are therefore hardly or rarely recalled in the brain.

**Anchoring/Adjustment-** Richter et al. 2018) - refers to a phenomenon that human assessments and decisions depend on initial values or starting values. These can be completely arbitrary and irrelevant to the decision. Thus, arbitrary numbers in the "back of the head" can be accessed, which influence the decision and play no role in the context. Influence on insurance decisions exists in that the current state is seen as the baseline for assessments of future deviations. These set anchors are then used to estimate variables relevant to the decision (Theil M. 2002 p. 90).



**Figure 1: Judgement heuristics**  
Theil M. 2002 p.55- 98 and Richter et al. 2018 p.8

In the depth interviews conducted by the researcher with doctors in the autumn of 2020, it has already been shown that doctors use these judgment heuristics. Representativeness and availability were shown in that the doctors did not recognize the threat to their own practice or did not consider it likely. Thus, they also have not contracted insurance to compensate for the damages of a cyber-attack. The current status is maintained as an anchor and insurance is not seen as necessary.

### III. RESULTS/ DECISION

Initial evaluations of the depth interviews already showed that due to the non-utilisation of insurance and justifications such as: "we have a software service provider who maintains the systems", "my practice is

too insignificant", "the server only runs under tags", "we are sufficiently protected", apparently the described heuristics were resorted to. These here then led to systematic errors, which in the end rejected insurance cover. This may be due to the fact that the probability of becoming a victim of a cyber-attack is classified as unlikely. Information that it could hit the doctor with his practice itself cannot be retrieved or is not imaginable. Similarly, that it could hit the "small, insignificant" medical practice is not perceived. Both judgement heuristics representativeness and availability are manifested, so that the current state (anchor) is maintained, and insurance is not taken out.

However, this is contradicted by the small number of doctors in depth-interviews studied and the advanced time of the first-time survey and publication of the GDV results in 2019.

It is planned to conduct online surveys in autumn 2021 with two associations: the German Association of Medical Specialists (Spitzenverband Fachärzte Deutschlands<sup>4</sup>) and the German Association of General Practitioners (Deutscher Hausärzterverband<sup>5</sup>). Both associations have interest, then the protection of physicians is important to them. An online survey will be conducted to investigate the attitudes of doctors towards insurance and towards the topic of cyber attacks and protection with a special insurance policy. This is to be tested once again to see whether it is once again apparent that doctors are subject to the judgment heuristics already described.

What is desirable is an increased risk awareness among doctors about the significance of cyber-attacks on their own medical practices. So, prevention analogous to the protective measures, wearing a mask, keeping a distance analogous to Corona. As well as increased insurance coverage, i.e., a better vaccination rate.

### REFERENCES

- [1] Art. 82 DSGVO – Haftung und Recht auf Schadenersatz. (2018, March 26). Datenschutz-Grundverordnung (DSGVO). <https://dsgvo-gesetz.de/art-82-dsgvo/>
- [2] Bechmann, G. (1993). *Risiko und Gesellschaft: Grundlagen und Ergebnisse interdisziplinärer Risikoforschung (German Edition)* (1993rd ed.). VS Verlag für Sozialwissenschaften.
- [3] GDV. (2019, May 31). *Branchenreport Cyberrisiken bei Ärzten und Apotheken*. [www.gdv.de](http://www.gdv.de). <https://www.gdv.de/resource/blob/45196/ae262d6702e2d9f5446c780a22450d23/download->

<sup>4</sup> [www.spifa.de](http://www.spifa.de)

<sup>5</sup> [www.hausaerzterverband.de](http://www.hausaerzterverband.de)

[branchenreport-cyber-aerzte-und-apotheker-data.pdf#page=1&zoom=70,-466,853](#)

- [4] Hiscox. (2021, April). *Hiscox Cyber Readiness Report 2021 - Don't let cyber be a game of chance*. (No. 5-). Hiscox Ltd.
- [5] Pfister, H., Jungermann, H., & Fischer, K. (2016). *Die Psychologie der Entscheidung: Eine Einführung (German Edition)* (4. Aufl. 2017 ed.). Springer.
- [6] Richter, Andreas/Jochen Ruß/Stefan Schelling: *Moderne Verhaltensökonomie in der Versicherungswirtschaft: Denkanstöße für ein besseres Verständnis der Kunden (essentials)* (German Edition), 1. Aufl. 2018., Wiesbaden, Germany: Springer Gabler, 2017.
- [7] Theil, M. (2002). *Versicherungsentscheidungen und Prospect Theory*. Springer Publishing.
- [8] Tversky, & Kahneman. (1974, September 27). *Judgment under Uncertainty: Heuristics and Biases*.  
[Http://Links.Jstor.Org](http://links.jstor.org).  
<https://www2.psych.ubc.ca/~schaller/Psyc590Readings/TverskyKahneman1974.pdf>