

Disclaimer: This paper is based on the facts surrounding the university hospital Düsseldorf cyberattack as known up to February 2021. Developments after that date have not been taken into consideration.

CASE STUDY FOR TOP EXECUTIVES, INCLUDING A CHECKLIST

3 rules for effective crisis PR after a cyberattack

How you protect your good reputation and win back your stakeholders' trust immediately

The invisible threat from the net is closing in. 50% of CEOs are deeply concerned about the danger coming from the internet, studies say (e.g. <https://www.pwc.com/ceosurvey.html>)

The concern of managers is justified. Switzerland is experiencing 98,000 cyberattacks as you read this, while Germany sees an incredible 2.2 million cyberattacks each year.

The question you should be asking yourself is not if there is an attack coming from the internet, but when it is going to happen. Can you do something against the looming reputational loss? Yes, you can.

We analyse an exemplary case, evaluate the crisis PR and make recommendations.

How dangerous are cyberattacks?

On 21 November 2020, German newspaper "Frankfurter Allgemeine Zeitung" (FAZ) wrote: "Düsseldorf learned in September that hacker attacks can literally endanger lives. After an attack on the university clinic's computer systems, emergency care was disrupted". An entire 14 days, emergency care was shut down. One patient had to be turned down – an odyssey in the ambulance followed and she died.

The attackers encrypted 30 servers of the university hospital, one of which contained a ransom note. "Until this day, clearing work is not done", FAZ wrote. The consequences of the attack: loss of turnover as well as costs for control and retrofitting. Plus the uncertainty as to whether sensitive data may have been stolen.

But what would be the worst possible damage for a company suffering such an attack? Clearly the loss of clients' trust.



Three rules for effective crisis PR

Rule no. 1: Be fast, and be event faster!

Let's assume that also your company has fallen victim to a cyberattack. What should you do first? Inform all stakeholders immediately. This way, you hold the reins and dictate the rhythm. Publish what you know as soon as you learn it. Whoever informs first is the most believable.

The case:

Düsseldorf reacted quickly to the attack during the night between the 9 and 10 September, more quickly than anyone else. Already at 07:08am, the communication department took to Twitter: "currently, the university clinic is experiencing a disruption of the IT system."

Rule no. 2: Inform clearly and regularly.

It's not what you say, but how you say it. Phrase your statements following an attack in a simple, concise, and unambiguous way. This way, you avoid whistleblowing. There's nothing to say at the moment? Inform about this as well. Share your strategy transparently in your communication and follow your own rules as well.

CHECKLIST: YOUR EMERGENCY STATEMENT IN FIVE STEPS

When making a statement in a crisis, stick to these guidelines:

- 1) Publish all known facts and their sources.
 - If necessary, use reported speech: "It was reported that the attack occurred during ..."
- 2) Share that there is nothing you can share; consider giving a reason.
 - "I cannot tell you any more at this point in time, because ..."
- 3) Show empathy, if appropriate – in a natural way, using your own words.
- 4) Share specifics: who's doing what exactly, and why?
 - Example: "The crisis team is meeting in order to ... / The next measures to be taken: ... / The investigation is led by ..."
- 5) By all means, announce when you'll be back with more.
 - Example: "We'll share more on the incident in the course of the morning."

The case:

The communication team of the Düsseldorf university clinic did indeed communicate clearly, on the website, Facebook, and Twitter. But not regularly enough on the first day. One Twitter user raised the legitimate question: “When will you provide more information?”

Uniklinik Düsseldorf @UniklinikDUS · 10. Sep. ⋮

Hinweis: Aktuell liegt im Universitätsklinikum Düsseldorf eine Störung des IT Systems vor. Das UKD ist daher momentan nur eingeschränkt erreichbar. Wir informieren darüber, wenn die Störung behoben ist. Vielen Dank für Ihr Verständnis.

Uniklinik Düsseldorf @UniklinikDUS · 11. Sep. ⋮

+++ Update 16 Uhr - Uniklinik Düsseldorf: Massiver Netzerkausfall +++ Krankenhaus derzeit nur eingeschränkt erreichbar – Patientenversorgung eingeschränkt – Möglicher Hackerangriff wird geprüft. Die komplette Pressemitteilung findet sich hier: uniklinik-duesseldorf.de/ueber-uns/pres...

Uniklinik Düsseldorf @UniklinikDUS · 14. Sep. ⋮


+++ Update (14. September 2020, 13.30 Uhr) +++ IT-Ausfall hält an: Patienten mit geplanten Behandlungsterminen werden gebeten, sich mit der jeweiligen Klinik oder Ambulanz in Verbindung zu setzen. Die Telefonverbindungen funktionieren wieder. +++ (1/3)

Uniklinik Düsseldorf @UniklinikDUS · 17. Sep. ⋮

+++ Update (17. September 2020, 10.00 Uhr) +++ Cyberangriff bestätigt – Sicherheitslücke in verbreiteter Software ermöglichte Zugang – Wiederherstellung geht Schritt für Schritt voran +++ (1/4)

Uniklinik Düsseldorf @UniklinikDUS · 18. Sep. ⋮

Stift und Papier sind gerade wichtige Werkzeuge bei uns auf dem Gelände... Auch uns im Twitter-Team stehen nur eingeschränkte Mittel zur Verfügung, aber wir haben mal ein kleines Dankeschön an unsere Kolleginnen und Kollegen gebastelt. Ihr seid wirklich unglaublich! (1/2)



Uniklinik Düsseldorf @UniklinikDUS · 20. Sep. ⋮

👍👍👍👍👍👍

Tom Luedde @tom_luedde · 20. Sep.

Die Mitarbeiter*innen der @UniklinikDUS lassen sich weder durch Hacker noch sonst irgend etwas davon abhalten, in schwierigen Zeiten zusammenzustehen und ihre Patient*innen exzellent zu versorgen. Ich ziehe meinen Hut und bin stolz, Teil dieses großartigen Teams zu sein!

🗨️ ↻️ ❤️ 20 📤

Uniklinik Düsseldorf @UniklinikDUS · 23. Sep. ⋮

+++ UPDATE (23. September 2020)+++ Uniklinik Düsseldorf wieder bereit für Notfälle +++ Nach IT-Ausfall werden weitere Systeme wieder in Betrieb genommen +++ Rettungsdienst kann UKD wieder anfahren +++ Planbare Behandlungen weiterhin gezielt abklären. +++ uniklinik-duesseldorf.de/nc/ueber-das-u...

The Twitter threads

Announcement: currently, the university clinic Düsseldorf is experiencing a disruption of the IT system. For this reason, the availability of UKD [university clinic Düsseldorf] is limited at the time. We will inform once the issue has been resolved. Thank you for your consideration.

+++ Update 4pm – university clinic Düsseldorf: massive network failure +++
Hospital availability limited currently – patient care limited – potential hacker attack is presently being investigated. Find the complete press release here: [link]

+++ Update (14 September 2020, 1:30pm) +++ IT disruption continues, patients with upcoming treatment dates are asked to contact the respective clinic or ambulance. Phone lines are back in service. +++ (1/3)

+++ Update (17 September 2020, 10am) +++ cyberattack confirmed – security vulnerability in widespread software allowed access – restoration is progressing step by step +++ (1/4)

Pen and paper are important tools on our premises right now... Also we from the Twitter team only have limited resources at our disposal, but we crafted a little thank you for our colleagues. You're truly incredible! (1/2)

❤️👉 ❤️👉 ❤️👉 ❤️👉 Tom Luedde

The employees of @UniklinikDUS are not letting themselves be stopped by a hacker or anything else in standing with each other during tough times and providing excellence care for their patients. I take my hat off to them and I am proud to be a part of this great team!

+++ UPDATE (23 September 2020) +++ University clinic Düsseldorf ready for emergency care again
+++ After IT outage, further systems are being taken back into operation +++ ambulance can access UKD again +++ Schedulable procedures still to be clarified specifically. +++ [link]

Rule no. 3: Do not downplay anything. Call things as they are!

If something happened: say only little, but as much as needed. Speak plainly! Say also what you don't know and who's going to do what until when: "We're currently investigating ..." This way, you can protect yourself from speculations. If rumours still go round, address them proactively.

The case:

On the day of the attack, 10 September 2020, the university clinic called the incident a "disruption of the IT systems" until 5pm. German news publication "Der Spiegel" was already reporting on a potential crime, referencing public prosecutor's office. In other words: the hospital may have shared less than they knew at the time, downplaying the facts.



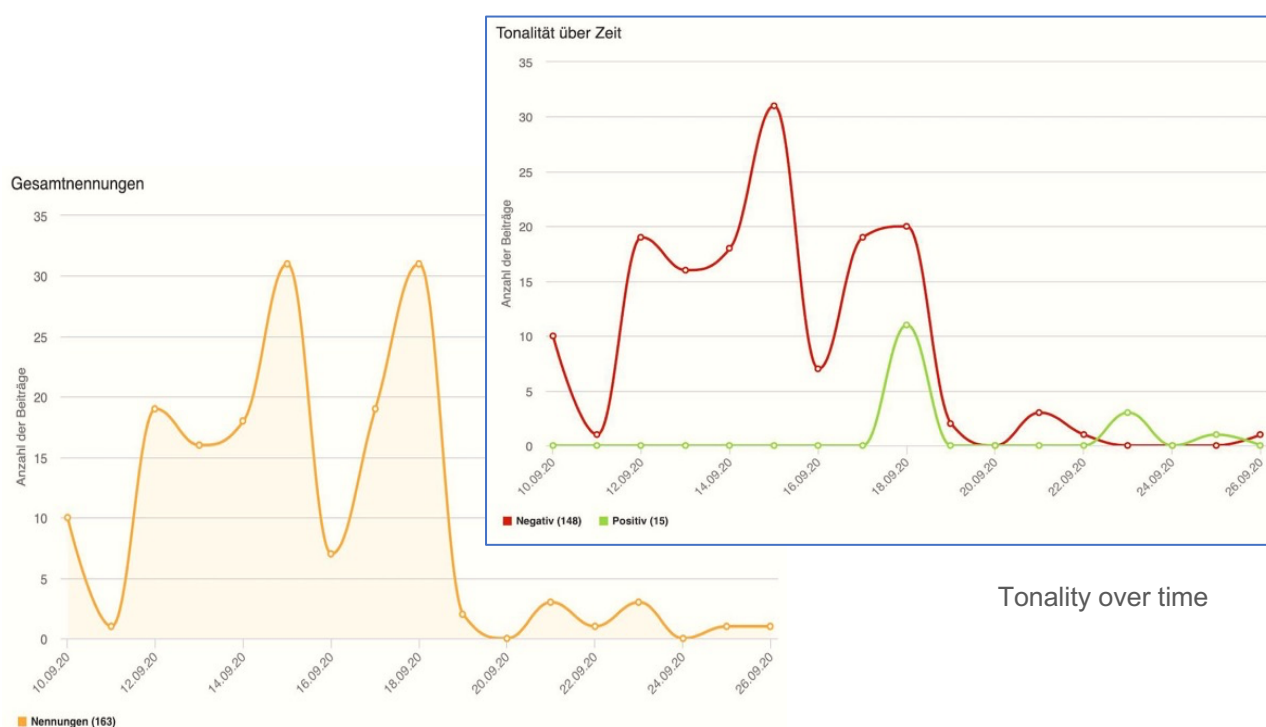
According to "Der Spiegel", a cyberattack is suspected (10 September 2020).

Why you should follow these three rules at all costs

Cyberattacks create a stir. Every new case demonstrates the vulnerability of our society and our economy. Sound communication helps you prevent damages.

The case:

From 10 September until 30 September, 160 statements were made spread across media and online forums, some of which were adopted as they stood by ten different publications. Naturally, the tonality of these statements was predominantly negative.



Tonality over time

Total mentions



Review: Communication in the university clinic case

The hospital's actions were commendable for the most part, instilling trust.

However:

- a) Media and the internet in general quickly offered more information than the company shared. A spokesperson of the central office for the prosecution of cybercrime at the Cologne public prosecutor's office stated on 10 September that "there is anecdotal evidence pointing towards criminal behaviour".

Problem & criticism: Why did the hospital not disseminate second-hand information itself?

- b) The attack was not without consequences: hundreds of patients were affected, and ambulance cars had to be redirected. Numerous headlines read "woman dies because of hacker attack". As it turned out later, she would have died regardless of the ambulance delay, but the word was out already.

Problem & criticism: Why did the hospital not show empathy or compassion with those affected? The Düsseldorf clinic did many things right. However, the silence on the emotional level sounded like guilt.

CHECKLIST: HOW DO YOU INFORM ABOUT CASUALTIES?

This sequence would be appropriate in a difficult situation:

- 1) Have there been fatalities?
- 2) How many seriously injured, and how many slightly injured people?
- 3) Has there been property damage?
- 4) Have operations been disrupted, or individual functions?
- 5) Have there been financial damages or consequences?

Advice & recommendations:

- Emotions are stronger than facts. Show compassion!
- Actions are stronger than facts, too. What would be a fitting symbolic gesture?
- You need sympathy! Send trustworthy people to the front.
- Address multipliers, including critics. Win them over as advocates!
- Your most important message is "we're taking care of it"