



FOR ORGANIZATIONS WITH MILLIONS OR BILLIONS TO PROTECT

The losses that start somewhere else

The most expensive incidents often begin outside the organization that pays for them: in a supplier's software, in a conflict between other countries, or in a counterparty whose numbers everyone else had already checked. These two cases show how that happens, what it cost, and the questions that would have been worth asking earlier.

[1. NotPetya and Maersk \(2017\)](#)

[2. Wirecard \(2020\)](#)

CASE STUDY 1 • CYBERATTACK • JUNE 2017

NotPetya: one software update, five continents

A destructive malware attack aimed at Ukraine spread through an ordinary accounting-software update and stopped one of the world's largest shipping companies, a major drugmaker, and a global courier within hours.

64+

countries with affected companies, according to Microsoft

\$10bn+

estimated total damage worldwide

\$200–300M

Maersk's own estimate of the impact on its results

49,000

PCs and servers Maersk reinstalled in 10 days

What happened

On June 27, 2017, malware later named NotPetya was pushed to organizations in Ukraine



through the automatic update of M.E.Doc, an accounting package widely used to file tax returns there. Once inside a network it spread on its own, using a Windows vulnerability called EternalBlue, for which Microsoft had released a patch in March 2017. It looked like ransomware, but it destroyed data rather than holding it for ransom.

Any company with an office in Ukraine that used the software became a way in. Global networks did the rest. A.P. Moller-Maersk, which its chairman later said handles roughly a fifth of world trade, lost its IT systems worldwide. Staff processed about 80% of the work by hand while the company reinstalled 45,000 PCs, 4,000 servers, and 2,500 applications in ten days.

How it spread across the economy

The disruption moved along supply chains. Maersk container terminals stalled on several continents. Merck reported lost sales of about \$135 million in the following quarter and borrowed Gardasil 9 vaccine from the US Centers for Disease Control's pediatric stockpile while production recovered. Trading in FedEx shares was briefly halted after its TNT Express unit was hit. In Pennsylvania, a hospital system could not offer lab and imaging services at 14 offices. Russia's own oil producer, Rosneft, was among the victims.

In February 2018 the US and UK governments attributed the attack to the Russian military. The White House called it "the most destructive and costly cyber-attack in history," which "quickly spread worldwide, causing billions of dollars in damage across Europe, Asia, and the Americas."

The second bill: insurance

Several victims then had to fight for their insurance. Insurers argued that a state-attributed attack fell under the "act of war" exclusion. Merck, which was reported to have suffered about \$1.4 billion in losses, won in New Jersey courts in 2023, which found the exclusion covered traditional warfare, and settled with its insurers in January 2024, more than six years after the attack.

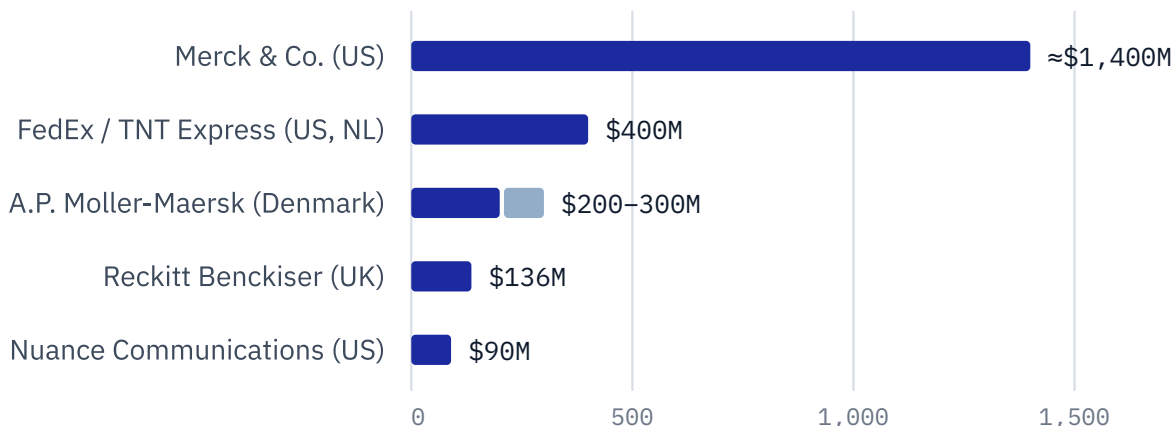
MAERSK TERMINALS REPORTED DISRUPTED	
EUROPE	Rotterdam, Netherlands; Spain
AFRICA	Morocco
ASIA	Mumbai (JNPT), India
S. AMERICA	Brazil; Argentina; Lima, Peru
N. AMERICA	Los Angeles; Elizabeth, New Jersey

As reported by Voice of America, June 30, 2017. Locations named in Maersk's update at the time; not a complete list.



Reported cost of NotPetya to selected companies

US dollars, millions, as each company or its reporting disclosed. Maersk reported a range; the lighter segment shows its upper end.



► [View as table](#)

Figures use different bases (lost revenue, costs, or total losses) and are not strictly comparable. Saint-Gobain (France) separately estimated less than €250 million in lost sales and €80 million in lost operating income for 2017.

You can be collateral damage

None of these companies was the main target. Operating in, or connecting to, a country in conflict brought the conflict into their networks.

Known vulnerabilities are the accelerant

A patch for the vulnerability that let NotPetya spread had been available since March 2017. Unpatched systems turned a local infection into a global one.

Trusted software is an entry point

The malware arrived through a legitimate vendor's update channel. A supplier's compromise became every customer's compromise.

Recovery and insurance are not guaranteed

Recovery took weeks of manual work, and some insurers disputed claims for years on the grounds that the attack was an act of war.

WHERE ACERVUS APPLIES

- **Exposure Assessment and Monitoring** watches an organization, its subsidiaries, and its portfolio companies from the outside for known exploited vulnerabilities, exposed remote access, and stolen credentials, the conditions that let an infection spread.
- **Cyber Incident Response** directs containment and eradication when an incident is underway, alongside the client's own IT staff.
- **Custom Solutions** address supplier and geographic exposure for clients with operations



in, or dependencies on, regions in conflict.

CASE STUDY 2 • CORPORATE FRAUD • JUNE 2020

Wirecard: €24 billion of market value, gone in a week

A German payments company that had joined the DAX, passed annual audits, and won investment from SoftBank collapsed after €1.9 billion of reported cash could not be found. The warning signs had been public for years.

€24bn

peak market value, 2018

€1.9bn

reported cash that could not be found

–97%

share price, June 17 to June 25, 2020

€900M

invested by SoftBank in 2019

What happened

Wirecard grew from a small payments processor into one of Germany's most valuable technology companies. Its shares rose from about €17 in 2013 to an all-time high in 2018, when it joined the DAX index of Germany's largest listed companies. Much of its reported profit came from partner companies in Asia that processed payments on its behalf.

On June 18, 2020, Wirecard announced that its auditor could not confirm €1.9 billion held in trust accounts, about a quarter of its balance sheet. The shares lost around 60% within minutes. The company then said the money most likely did not exist, and on June 25 it filed for insolvency, the first DAX member to do so. The shares closed that day at €3.50 and fell below €1 by late August.

The signs that were already public

Journalists, short sellers, and later a special auditor had raised specific questions for five years. Each time, the share price fell and recovered, and the company, its auditor, and Germany's financial regulator BaFin pushed back on the critics. In 2019 BaFin temporarily banned short selling of the stock, and authorities investigated journalists who had reported on the company.



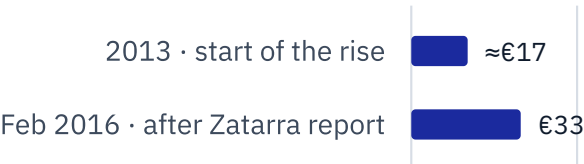
Aftermath

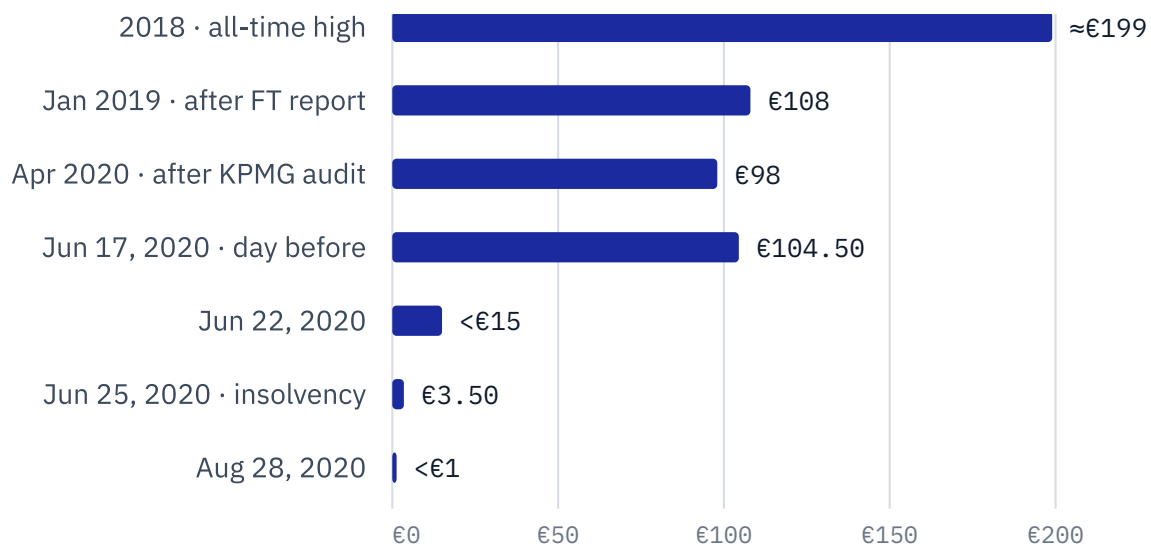
Former CEO Markus Braun was arrested in June 2020. His criminal trial in Munich began in December 2022; he has denied the charges. Former chief operating officer Jan Marsalek disappeared after the collapse and is the subject of an Interpol Red Notice. The head of BaFin and his deputy left the regulator in January 2021. Courts in Singapore and the United States have sentenced people connected to the case, and a German court ordered former board members to pay €140 million in damages.

PUBLIC WARNING SIGNS	
Apr 2015	Financial Times "House of Wirecard" column questions its accounts
Feb 2016	Zatarra Research report; shares fall from €42 to €33
Jan 2019	FT reports suspected forged and backdated contracts in Singapore; shares fall from €167 to €108 in two days
Feb 2019	Singapore police search Wirecard's offices; BaFin bans short selling for two months
Apr 2020	KPMG special audit cannot verify most 2016–2018 profits; shares fall from €132 to €98
Jun 18, 2020	€1.9 billion in cash cannot be confirmed
Jun 25, 2020	Insolvency filing

Wirecard share price at key moments

Euros per share. Selected prices reported at each event, not a continuous daily series.





► [View as table](#)

The 2018 high is approximate. Sources: LUISS working paper on Wirecard and BaFin (2021); FXStreet, June 30, 2020.

Credentials are not verification

An index listing, clean audit opinions, a supervising regulator, and a famous investor all signaled legitimacy. None of them confirmed that the cash existed.

Pushback is not a rebuttal

Lawsuits against critics, regulatory action against short sellers, and confident denials kept investors in the stock. They did not answer the questions.

The questions were answerable from outside

The critical questions were whether the partner companies were real businesses and whether the reported money was where the company said it was. Reporters pursued those questions from public records and on-the-ground checks.

Losses arrive faster than exits

Shareholders had five years of warnings and one week of collapse. Once the cash was declared missing, there was no orderly way out.

WHERE ACERVUS APPLIES

- **Investigative Analytics** verifies, independently and from the outside, whether counterparties, partners, and the people behind them are what they claim to be.
- **Private Equity & M&A diligence** brings those questions forward, before a commitment is signed rather than after a collapse.
- **Custom Solutions** are built for clients whose exposure, jurisdiction, or sensitivity calls for work beyond a standard engagement.



OUR EXPERIENCE

Acervus has applied its Investigative Analytics and Custom Solutions to matters of this kind for past clients.

Client work is confidential. Examples are available to vetted clients on request. Acervus was not involved in the events described in these case studies, which are drawn entirely from public reporting.

Request a consultation

SOURCES

1. Voice of America, "Companies Still Hobbled From Fearsome Cyberattack," June 30, 2017 (64 countries per Microsoft; terminals; Heritage Valley; FedEx trading halt).
2. The Bulletin of the Atomic Scientists, "The worst cyberattack so far," August 2018 (more than \$10 billion in total damage).
3. Help Net Security, "NotPetya aftermath: Companies lost hundreds of millions," August 17, 2017 (Maersk; Saint-Gobain).
4. SecurityWeek, "Maersk Reinstalled 50,000 Computers After NotPetya Attack," January 2018 (Snabe figures).
5. SecurityWeek, "NotPetya Attack Had Significant Impact on Merck Revenue," October 2017; Infosecurity Magazine, "Merck Settles With Insurers Over \$700m NotPetya Claim," January 8, 2024.
6. The Security Ledger, "NotPetya's Cost to FedEx: \$400 Million and Counting," December 22, 2017; The Register, NotPetya anniversary, June 27, 2018 (Reckitt Benckiser); SecurityWeek, "Nuance Estimates NotPetya Impact at \$90 Million."
7. eWeek, "U.S. Formally Accuses Russia of Launching NotPetya Ransomware Attack," February 2018 (White House and UK statements).
8. Wikipedia, "Wirecard scandal" (timeline, €24bn peak, €1.9bn, SoftBank, BaFin, Marsalek); Financial Times reporting, 2015–2020.
9. LUISS School of European Political Economy, "The Wirecard scandal and the role of BaFin," working paper (share prices at events).
10. FXStreet, June 30, 2020 (June 2020 high); Malay Mail, June 25, 2020 (first DAX member to file for insolvency); Wikipedia, "Markus Braun"; Baker McKenzie Global Litigation News, January 3, 2025 (€140 million).



