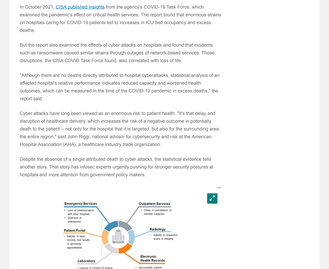

FEATURE

Studies show ransomware has already caused patient deaths

No patient deaths have been definitively attributed to cyber attacks on hospitals, but some infosec experts say that statistical evidence shows a different, grim reality.

By Alexis Zachariadou, Student Co-op

When it comes to ransomware attacks on hospitals, the subject of patient deaths has typically been a hot potato.

As threat of ransomware has increased in recent years, news reports of hospitals and medical facilities suffering outages and significant service disruptions have become a weekly occurrence. Government officials and healthcare experts across the globe have long warned that such cyber attacks will eventually cause loss of life.

There have already been relatable incidents where cyber attacks were implicated in patient deaths. For example, a 2019 ransomware attack on Springhill Medical Center in Alabama caused facility further led to a newborn's death, according to a lawsuit filed against the hospital. The Wall Street Journal called the incident "the first alleged ransomware death." though no criminal charges were filed and the lawsuit is still pending.

More recently, authorities in Germany investigated a 2020 ransomware attack against Düsseldorf University Hospital as a potential case of negligent homicide. Disruptions to the hospital caused a 78-year-old patient to be diverted to another facility further away, where she later died. However, German police ultimately concluded that a "causal link" between the attack and the patient's death could not be established.

But some infosec experts say that Rubicon was passed years ago – we just haven't come to grips with it yet. Such experts point to recent studies that show cyber attacks on healthcare organizations have increased patient mortality. While those infosec experts hope that the results from increased government notification will improve security in medical devices, there's a separate concern about an unwillingness to fully acknowledge what recent studies and statistical evidence have shown.

In October 2021, CISA published insights from the agency's COVID-19 Task Force, which examined the pandemic's effect on critical health services. The report found that enormous strains on hospitals caring for COVID-19 patients led to increases in ICU bed occupancy and excess deaths.

But the report also examined the effects of cyber attacks on hospitals and found that incidents such as ransomware caused similar strains through outages of critical systems. Those disruptions, the CISA-COVID Task Force found, also correlated with loss of life.

"Although there are no deaths directly attributed to hospital cyberattacks, statistical analysis of an affected hospital's relative performance indicates reduced capacity and worsened health outcomes, which can be measured in the time of the COVID-19 pandemic in excess deaths," the report said.

Cyber attacks have long been viewed as an enormous risk to patient health. "It's that delay and disruption to healthcare delivery that increases the risk of a negative outcome, potentially death to the patient – not only for the hospital that it is targeted, but also for the surrounding area, the entire region," said John Riggi, national advisor for cybersecurity and risk at the American Hospital Association (AHA), a healthcare industry trade organization.

Despite the absence of a single attributed death to cyber attacks, the statistical evidence tells another story. That story has infosec experts urgently pushing for stronger security postures at hospitals and more attention from government policy makers.

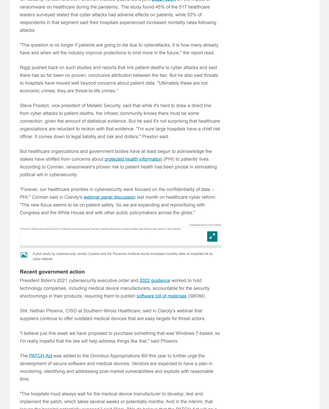

Figure 8 – Hospital System Services and Departments Disrupted by Cyber Attack

A 2021 report from CISA's COVID Task Force found that cyber attacks on hospitals caused enormous strain on healthcare staff and services, leading to excess deaths in those regions.

Studies on cyber-related loss of life

When it comes to emergency medical care, it's all about time and distance. A study released in 2017 investigating the impacts of prolonged care delivery during major U.S. marathons found that the average ambulance travel time increased about 32% on marathon days in comparison to non-marathon days. Moreover, higher mortality rates were recorded for those admitted on race days.

For a patient having a heart attack, receiving care in 4.4 minutes is often the difference between life and death. A widely known concept in medical care called the "Golden Hour," first introduced in the 1950s, argues that survival rates following a traumatic injury begin to plummet if medical care isn't provided within an hour of the injury (though some medical experts today say the concept lacks validity). In the event of delayed medical care, or disrupted healthcare operations – those who require help within hours or minutes often do not receive it.

Ransomware attacks often prolong the wait for medical assistance. In the 2017 WannaCry attacks, which infected hundreds of thousands of systems worldwide, caused significant disruptions for the U.K.'s National Health Service facilities. Thousands of appointments were cancelled across several regions, and patients were forced to travel much further to received treatment.

Joshua Corman, *previous chief strategist* of the CISA COVID Task Force and vice president of cyber safety strategy at Claroty, said "it's impossible people didn't die" during the WannaCry attacks because of the healthcare disruptions.

"What we know is that delays affect mortality. And what we can show with many of these attacks is that the unavailability of a device or hospital and the diversion of ambulances can introduce delays of minutes or hours or days or weeks," Corman said.

During the early stages of the pandemic, the CDC observed that the number of deaths exceeded the predicted volume the virus would yield. Excess deaths resulted from non-COVID-19 deaths or other losses of life that stemmed from strained healthcare services and operations.

> **Ultimately, these are not economic crimes; they are threat to life crimes.**
>
> **John Riggi**
> National advisor for cybersecurity and risk at the American Hospital Association

CISA experts on the COVID Task Force then correlated the volume of deaths documented in hospitals unaffected and those that were affected by ransomware. The analysis revealed that regions hit by ransomware experienced excess death stress levels sooner and for a longer period than unaffected peers in their state.

Studies gauging the collateral damage of these attacks are still being published. Cyneric, a health IoT security vendor, and the Ponemon Institute published a 2022 report on the impact of ransomware on healthcare during the pandemic. The study found 43% of the 617 healthcare leaders surveyed stated that cyber attacks had adverse effects on patients, while 53% of respondents in that segment said their patients died because of ransomware-related following attacks.

"The question is no longer if patients are going to die due to cyberattacks, it is how many already have and when will the industry improve protections to limit more in the future," the report read.

Riggi pushed back on such studies and reports that link patient deaths to cyber attacks and said there has so far been no proven, conclusive attribution between the two. But he also said that threats to hospitals have moved well beyond concerns about patient data. "Ultimately these are not economic crimes; they are threat-to-life crimes."

Steve Preston, vice president of Metallic Security, said that while it's hard to draw a direct line from cyber attacks to patient deaths, the infosec community knows there must be some connection, given the amount of statistical evidence. But he said it's not surprising that healthcare organizations are reluctant to reckon with that evidence. "I'm sure large hospitals have a chief risk officer. It comes down to legal liability and risk and dollars," Preston said.

But healthcare organizations and government bodies have at least begun to acknowledge the stakes have shifted from concerns about protected health information (PHI) to patients' lives. According to Corman, ransomware's proven risk to patient health has been pivotal in stimulating political will in cybersecurity.

"Forever, our healthcare priorities in cybersecurity were focused on the confidentiality of data – PHI," Corman said in Claroty's webinar panel discussion last month on healthcare cyber reform. "The new focus seems to be on patient safety. So we are expanding our partnership with Congress and the White House and with other public policymakers across the globe."

A joint study by cybersecurity vendor Cynerio and the Ponemon Institute found increased mortality rates at hospitals hit by cyber attacks.

Recent government action

President Biden's 2021 cybersecurity executive order and 2022 guidance worked to hold technology companies, including medical device manufacturers, accountable for the security shortcomings in their products, requiring them to publish software bill of materials (SBOM).

Still, Nathan Phoenix, CISO at Southern Illinois Healthcare, said in Claroty's webinar that suppliers continue to offer outdated medical devices that are easy targets for threat actors.

"I believe just this week we have proposed to purchase something that was Windows 7-based, so I'm really hopeful that the law will help address things like that," said Phoenix.

> **What we know is that delays affect mortality. And what we can show with many of these attacks is that the unavailability of a device or hospital and the diversion of ambulances can introduce delays of minutes or hours or days or weeks.**
>
> **Josh Corman**
> Vice president of cyber safety strategy, Claroty

The PATCH Act was added to the Omnibus Appropriations Bill this year to further urge the development of secure software and medical devices. Vendors are expected to have a plan in monitoring, identifying and addressing post-market vulnerabilities and exploits with reasonable time.

"The hospitals must always wait for the medical device manufacturer to develop, test and implement the patch, which takes several weeks or potentially months. And in the interim, that leaves the hospital potentially exposed," said Riggi. "We do believe that the PATCH Act will go a long way in helping reduce the risk the cyber risk associated with medical devices."

But healthcare executives say it will take time for hospitals across the nation to adopt new practices.

"That's one of the real challenges with this. The act has to basically be then built out into a structure to support this, and we know there's still going to be resistance – there's going to be confusion," said Jennings Aske, chief information officer at New York Presbyterian Hospital, in a statement.

The Biden administration's 2023 National Cybersecurity Strategy augments the past executive actions in pressuring sellers. The strategy proposed that failing to meet minimum cyber hygiene requirements will be met with legal civil liability.

The strategy also places priority on dismantling threat actors' operations. By working with the government, the administration plans to take an offensive role against adversaries in the name of a "safe and secure digital ecosystem for all Americans."

The government has already initiated several operations in combating cybercrime. For example, in January the FBI infiltrated the Hive ransomware gang's network and ultimately seized their servers and decryption keys, providing relief for several victims.

Will legislation provide relief?

Though the government has slowly recognized the severity of the situation, experts say it will be especially difficult for the healthcare sector to make reforms due to financial restraints and lack of resources.

"You can push as many requirements on hospitals as you want, and they're going to figure out a way to work with them," said Chad Holmes, security evangelist at Cynerio. "But if you don't provide them expertise, if you don't provide them funding, if you don't provide them, people, they're not going to be effective."

The shortage of security professionals has impacted many vertical industries but has also presented major challenges to healthcare organizations' ability to adopt and maintain best practices. In addition, adhering to new laws and regulations demands sufficient IT and infosec staffing in hospitals.

"As a country, we know we have a deficit of workers who can help us defend our enterprises. So how do we think differently than we ever have before? Where do we find folks who have the attitude, the curiosity, the ability?" said Greg Garneau, CISO at Mansfield Oil Company of Gainesville, Texas, during the webinar panel. "As a nation, we really need to start thinking much differently about how we staff because that is obviously a very weak link."

While protecting patients' lives is imperative, improving security postures in healthcare organizations and staving off the steady flow of disruptive cyber attacks is an uphill battle. The webinar panelists said significant improvements will require significant cooperation with the U.S. government, which has been shaky in the past. But it may be the only way to provide hospitals the ongoing threats and enact lasting improvements.

"Mandating things is difficult sometimes, especially when you don't have the time or talent or funding but you also want some relief," said Garneau. "There is a place for the federal government to assist us to provide relief."

This was last published in May 2022

Related Resources
NIH, Pay to security and business success in the digital era
TechTarget ComputerWeekly.com
Information Security Threats: Building Risk Resilience
TechTarget Security
Towards an Autonomous Vehicle Enabled Society: Cyber Security Implications
TechTarget ComputerWeekly.com
April Essential Guide to Data Protection
TechTarget Security