

# The Good, The Bad, and The Ugly of Cybersecurity

YOUR PARTNER FOR HEALTHY  
**CHANGE**



Bill Phillips  
EVP, Chief Information Officer  
University Health  
[Bill.Phillips@uhtx.com](mailto:Bill.Phillips@uhtx.com)

Serina Rivela  
VP/Chief Legal Officer  
University Health  
[Serina.Rivela@uhtx.com](mailto:Serina.Rivela@uhtx.com)



## Change Healthcare

### HHS intervenes in Change Healthcare hack

[HHS intervenes in Change Healthcare hack \(TheCockfield.com\)](#)

HHS said March 5 it would help accelerate payments to hospitals affected by the Change Healthcare cyberattack and institute other workarounds for providers.

HEALTH CARE Published February 22, 2024 12:10pm EST

### Pharmacies nationwide report outages in wake of cyberattack

Change Healthcare said it became aware of the 'outside threat' on Wednesday morning, disconnecting their systems for security purposes

### THA, AHA Push for More Help on Cyberattack, Seek Hospital Data

THA and the American Hospital Association are continuing work to help membership sort out the implications of the Optum/Change Healthcare cyberattack this week as the federal government announced flexibilities for hospitals to account for the breach – steps that AHA deemed to be an inadequate response.

The Feb. 21 ransomware attack on Change Healthcare – part of Optum and owned by UnitedHealth Group – is believed to have been perpetrated by the [cybercrime group](#) known as BlackCat or ALPHV, according to reports. Change handles a reported 15 billion health care transactions per year and touches one of every three patient records.

Suspected nation-state associated cyber security threat actor

### BlackCat Reportedly Behind Change Healthcare Incident

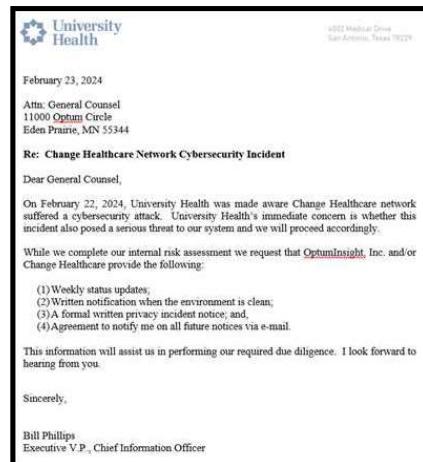
The BlackCat group has reportedly claimed responsibility for the [ongoing cyber-attack against Change Healthcare](#), stating on its dark web site that it exfiltrated GTB of data from the firm. However, the claim was subsequently removed without explanation.

#### Action:

- Severed all connections and blocked domains
- Communicated impact to our organization
- Sent letter to Change Healthcare
- Monitor daily

The U.S. Department of Health and Human Services' Office for Civil Rights (OCR) just announced an [investigation](#) into the recent cyberattack that affected Change Healthcare.

Cyber threats of this magnitude are on the rise, with over [134 million](#) individuals impacted by breaches in 2023, a 141% increase from 2022.



# BlackCat



## BlackCat Adapts Techniques Following Law Enforcement Operation

The advisory said that BlackCat actors are employing improvised communication methods by creating victim-specific emails to notify of the initial compromise.

For example, affiliates offer to provide unsolicited cyber remediation advice as an incentive for making a payment, such as "vulnerability reports" and "security recommendations" to prevent future attacks.

- The US government has warned the healthcare sector that it is now the biggest target of the BlackCat ransomware group.
- The joint advisory from the FBI, the Cybersecurity and Infrastructure Security Agency (CISA) and the Department of Health and Human Services (HHS), noted of the nearly 70 leaked victims of BlackCat since mid-December 2023, healthcare has been the most commonly victimized industry.
- This follows a post by a BlackCat administrator encouraging affiliates to target hospitals in early December in response to [law enforcement action](#) taking down the Russian-speaking group's leak site.
- The group [appeared to "unseize"](#) its leak site shortly after the announcement.
- BlackCat, also known as ALPHV, is reportedly behind the ongoing cyber incident affecting health tech firm Change Healthcare, which was first reported on February 21.



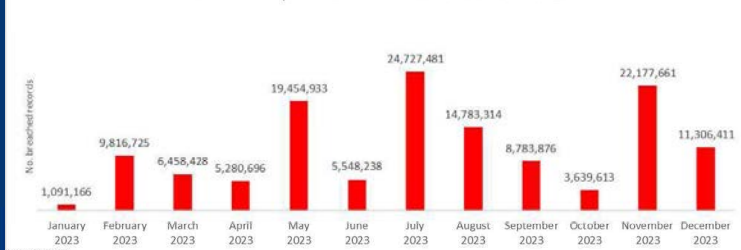
# 2023 Healthcare Data Breaches

- More than 2,600 organizations worldwide had data stolen in the attacks, with the healthcare industry among the worst affected
- 95% of all identity theft incidents reportedly come from compromised healthcare records
- Phishing attacks were used as the first stage of an attack. 45% of all successful data breaches in healthcare were due to phishing

## Top 10 Organizations Affected

| Name of Covered Entity                                | State | Covered Entity Type | Individuals Affected | Cause of Data Breach                     |
|---|-------|---------------------|----------------------|--|
| HealthEC LLC  | NJ    | Business Associate  | 4,452,782            | Hacking incident (Data theft confirmed)  |
| ESO Solutions, Inc.                                   | TX    | Business Associate  | 2,700,000            | Ransomware attack                        |
| Transformative Healthcare (Fallon Ambulance Services) | MA    | Healthcare Provider | 911,757              | Hacking incident (Data theft confirmed)  |
| Electrostim Medical Services, Inc. dba EMSI           | FL    | Healthcare Provider | 542,990              | Hacking incident                         |
| Cardiovascular Consultants Ltd.                       | AZ    | Healthcare Provider | 484,000              | Ransomware attack (Data theft confirmed) |
| Retina Group of Washington, PLLC                      | MD    | Healthcare Provider | 455,935              | Ransomware attack                        |
| CompleteCare Health Network                           | NJ    | Healthcare Provider | 313,973              | Ransomware attack (Data theft confirmed) |
| Health Alliance Hospital Mary's Avenue Campus         | NY    | Healthcare Provider | 264,197              | Hacking incident (Data theft confirmed)  |
| Independent Living Systems, LLC                       | FL    | Business Associate  | 123,651              | Hacking incident (MOVEit)                |
| Pan-American Life Insurance Group, Inc.               | LA    | Health Plan         | 105,387              | Hacking incident (MOVEit)                |
| Meridian Behavioral Healthcare, Inc.                  | FL    | Healthcare Provider | 98,808               | Hacking incident                         |

Records Compromised in Healthcare Data Breaches



# Why Target Healthcare

- Contains a greater and broader amount of personal information, more than employers or banks
- Serves as a larger pool of potential victims
- Financial data has a finite lifespan, healthcare information lives forever
- PHI can be monetized and exploited
- PHI is 10-70x more valuable than credit card information

The medical records of patients can sell for as much as **\$1,000 on the dark web.**

The black market value of medical records stands at **\$250 (on average).**

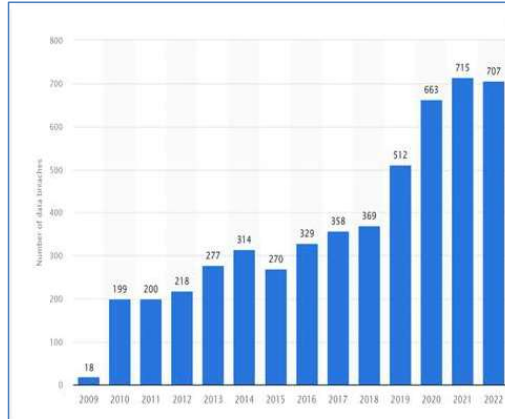
Medical records are valuable because they contain lots of sensitive data, which cannot be changed easily by victims.

This means the percentage of breaches classed as 'theft or loss' is much higher in the healthcare industry than in other sectors.

**'Theft or loss' data breaches:**

|                     |     |
|---------------------|-----|
| Other industries    | 15% |
| Healthcare Industry | 32% |

SafetyDetectives



Healthcare Data Breaches

From 2023 to 2032, the healthcare cybersecurity market is expected to swell...

Healthcare Cybersecurity will grow **18.5% year-on-year.**

The market value is projected to reach **\$92 billion by 2032.**

SafetyDetectives

**\$10,600**  
Downtime cost per minute for Healthcare organizations clinical systems

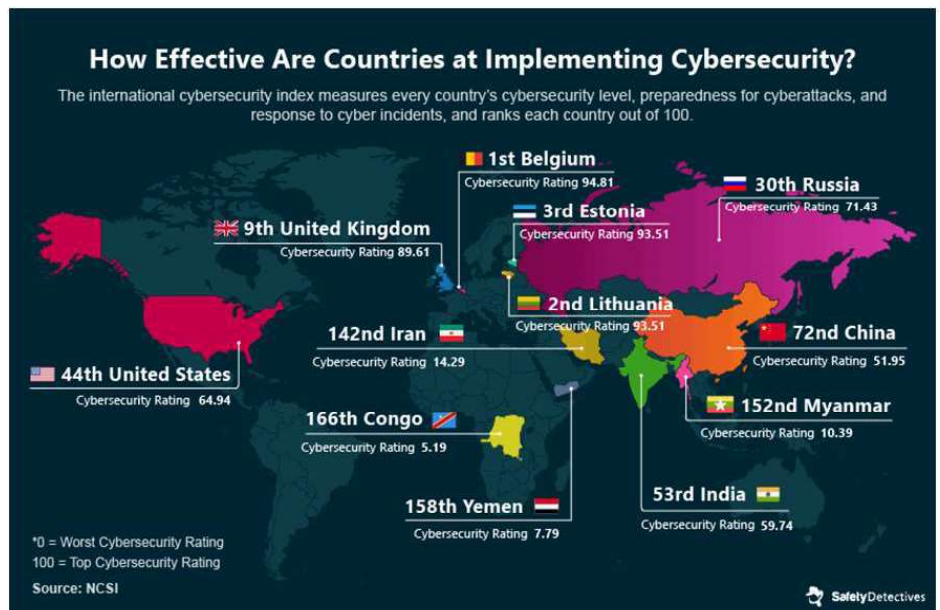


5

# Cybersecurity Rating by Nation

So, which countries are best placed to deal with cybersecurity incidents in healthcare?

The national cybersecurity index measures a nation's cybersecurity level, preparedness for cyberattacks, and response to cyber incidents.



6

Find the full text of this and thousands of other resources from leading experts in dozens of legal practice areas in the [UT Law CLE eLibrary \(utcle.org/elibrary\)](http://utcle.org/elibrary)

Title search: The Good, The Bad, and The Ugly of Cybersecurity

Also available as part of the eCourse

[eSupplement to the 40th Annual School Law Conference](#)

First appeared as part of the conference materials for the  
35<sup>th</sup> Annual Health Law Conference session

"The Good, The Bad, and The Ugly of Cybersecurity"