CyberPeace Institute

Tracking Cyberttacks against the Healthcare Sector

CyberIncident Tracer#HEALTH

Francesca Bosco

The CyberPeace Institute

- Independent NGO, launched 2019
  - Due to escalating dangers of cyberattacks
- Founding partners
  - Microsoft, Hewlett Foundation, Mastercard & others
- HQ in Geneva
  - 33 FTEs (as of Dec 2021)
  - 13 nationalities
  - 52% women - 48% men
- Strategic objectives
  - Assistance
  - Analysis
  - Advancement
  - Foresight and Capacity Building

CyberPeace Institute PUBLIC // TLP: White

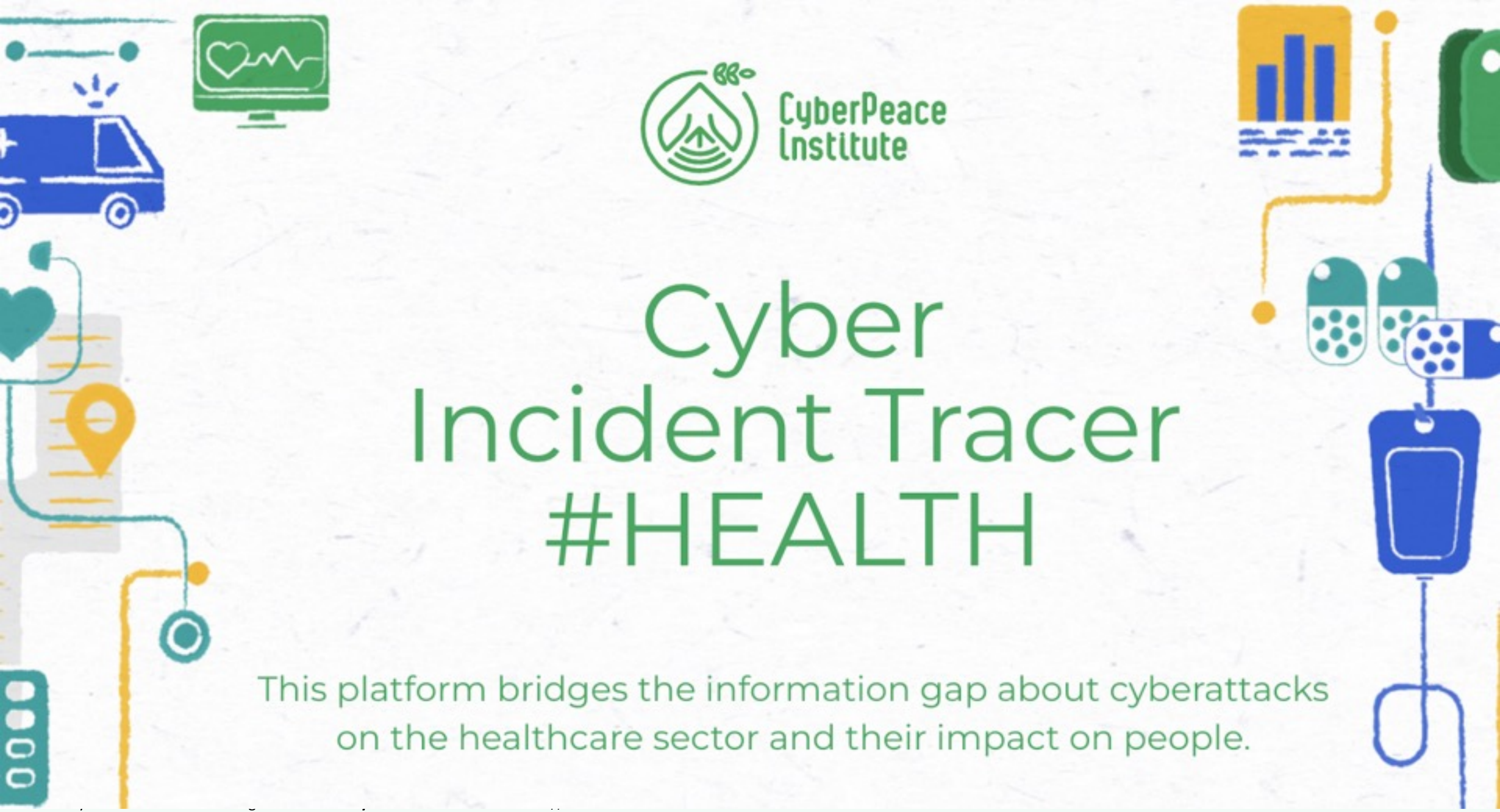
A brief history

2020	May	**Call to Governments** To stop cyberattacks on the healthcare sector
	June	**Cyber 4 Healthcare** Cybersecurity-healthcare matchmaking service
2021	March	**Playing with Lives** Strategic analysis report on cyberattacks on the healthcare sector
	October	**Cyber Incident Tracer #HEALTH** Platform and microsite launch
	October	**CyberPeace Builders** A network of corporate volunteers providing free assistance to NGOs
2022	July	**Compendium** Protecting the Healthcare Sector from Cyber Harm (with MSFT, Czech Republic)

March 2021

Playing with Lives: Cyberattacks on Healthcare are Attacks on People

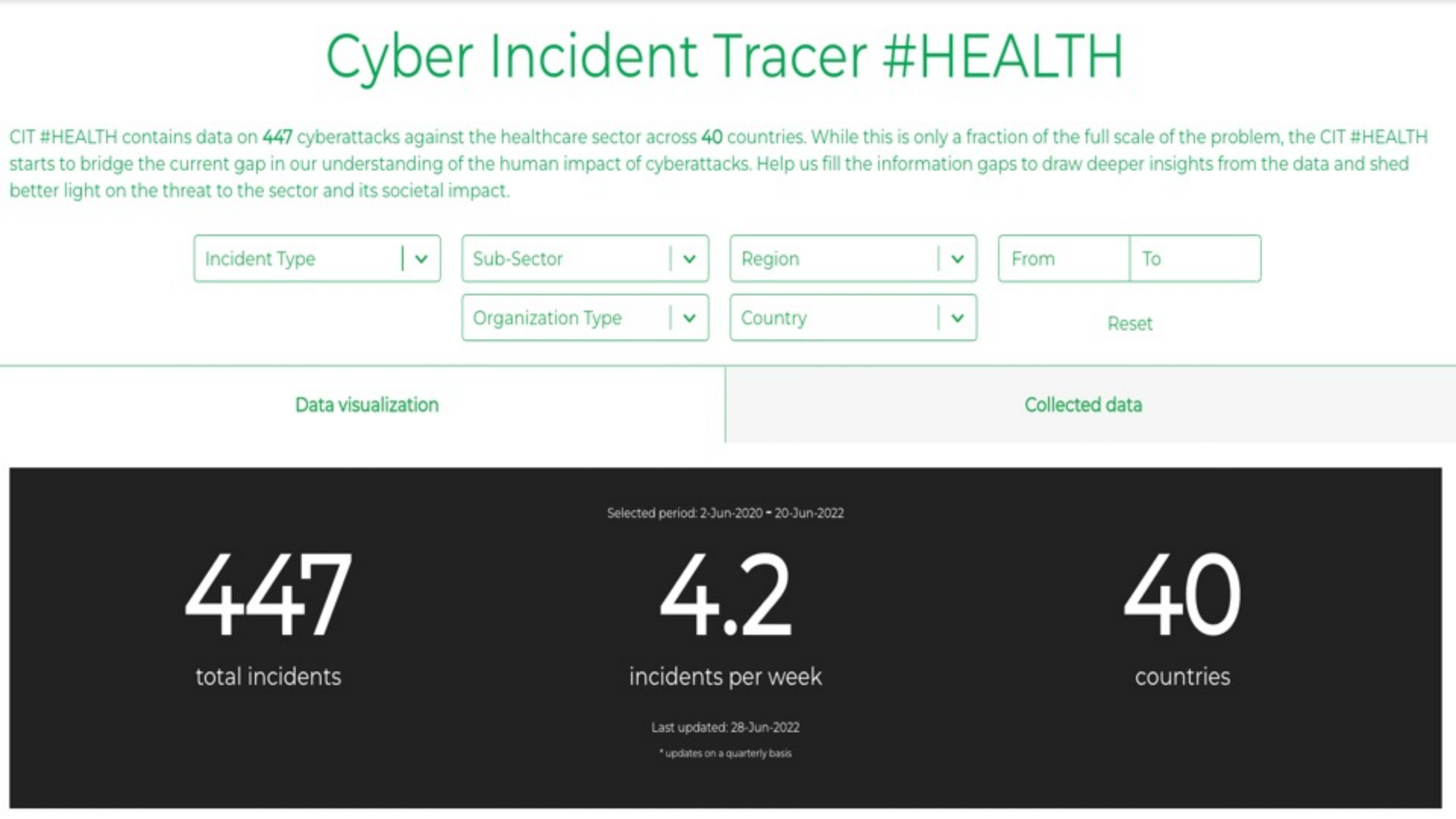
The CyberPeace Institute



CyberPeace Institute

Cyber Incident Tracer #HEALTH

This platform bridges the information gap about cyberattacks on the healthcare sector and their impact on people.



Cyber Incident Tracer #HEALTH

CIT #HEALTH contains data on **447** cyberattacks against the healthcare sector across **40** countries. While this is only a fraction of the full scale of the problem, the CIT #HEALTH starts to bridge the current gap in our understanding of the human impact of cyberattacks. Help us fill the information gaps to draw deeper insights from the data and shed better light on the threat to the sector and its societal impact.

Selected period: 2-Jun-2020 - 20-Jun-2022

447
total incidents

4.2
incidents per week

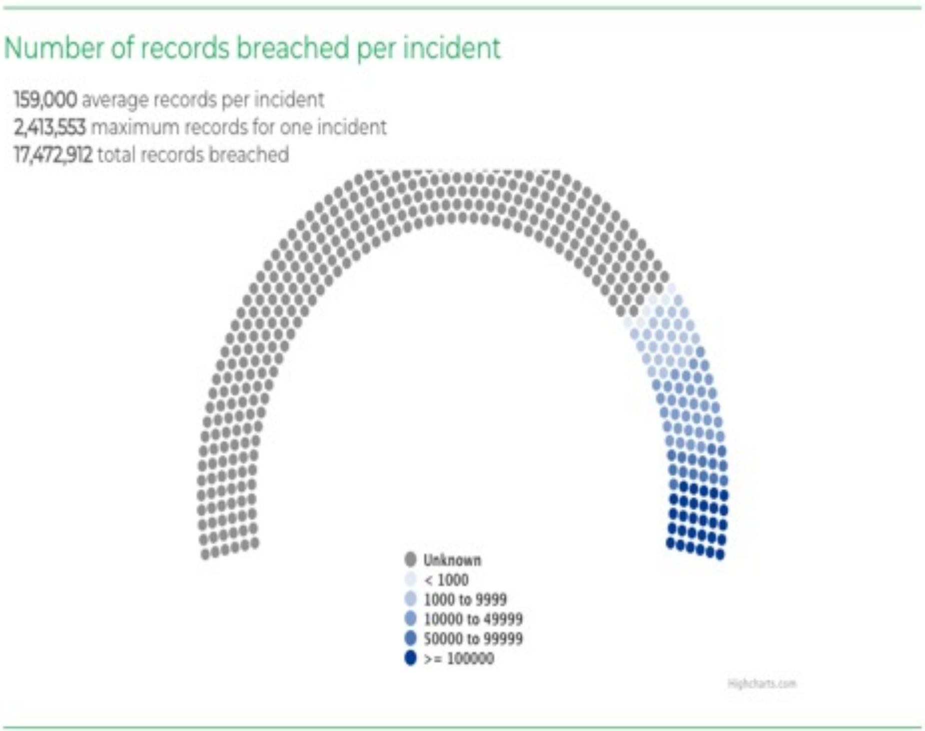
40
countries

Last updated: 28-Jun-2022

* updates on a quarterly basis

Impact and harm

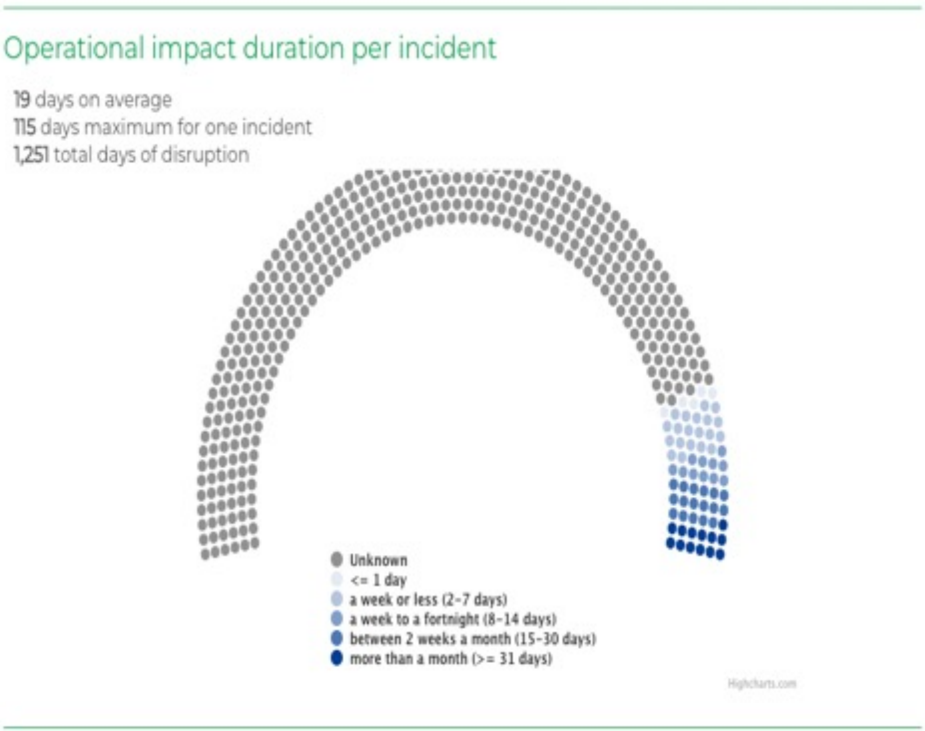
on Individuals



Number of records breached per incident

159,000 average records per incident
2,413,553 maximum records for one incident
17,472,912 total records breached

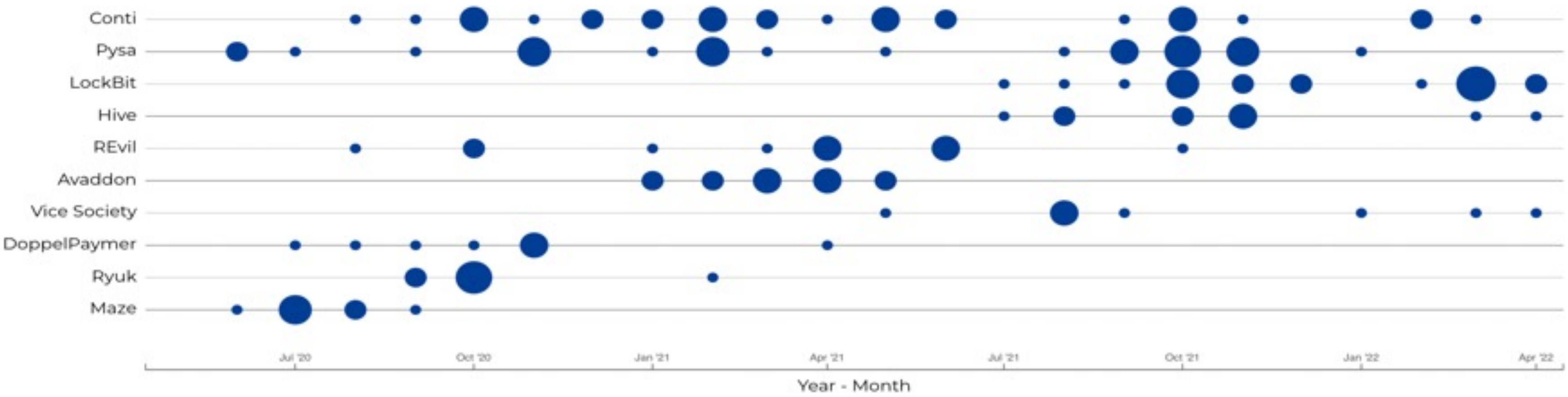
on Organizations



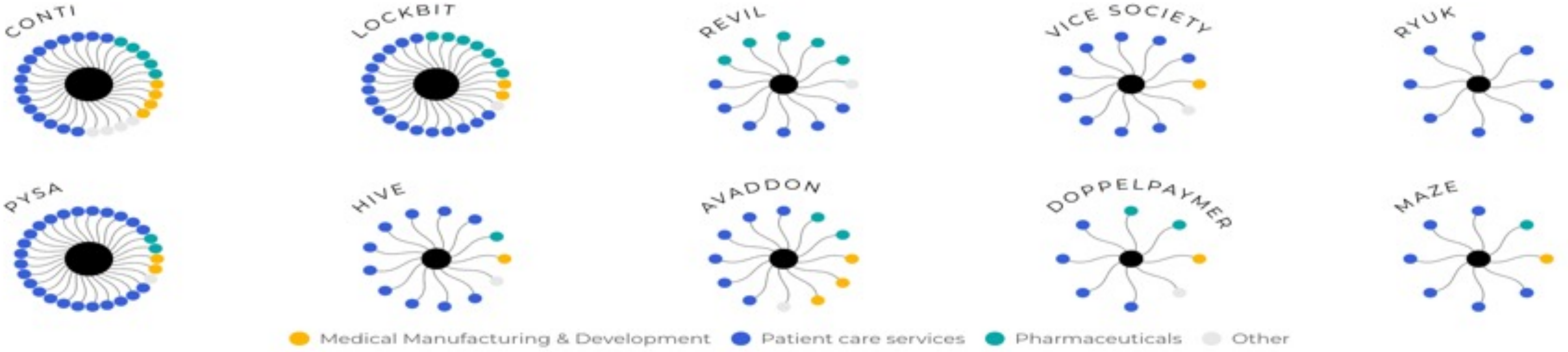
Operational impact duration per incident

19 days on average
115 days maximum for one incident
1,251 total days of disruption

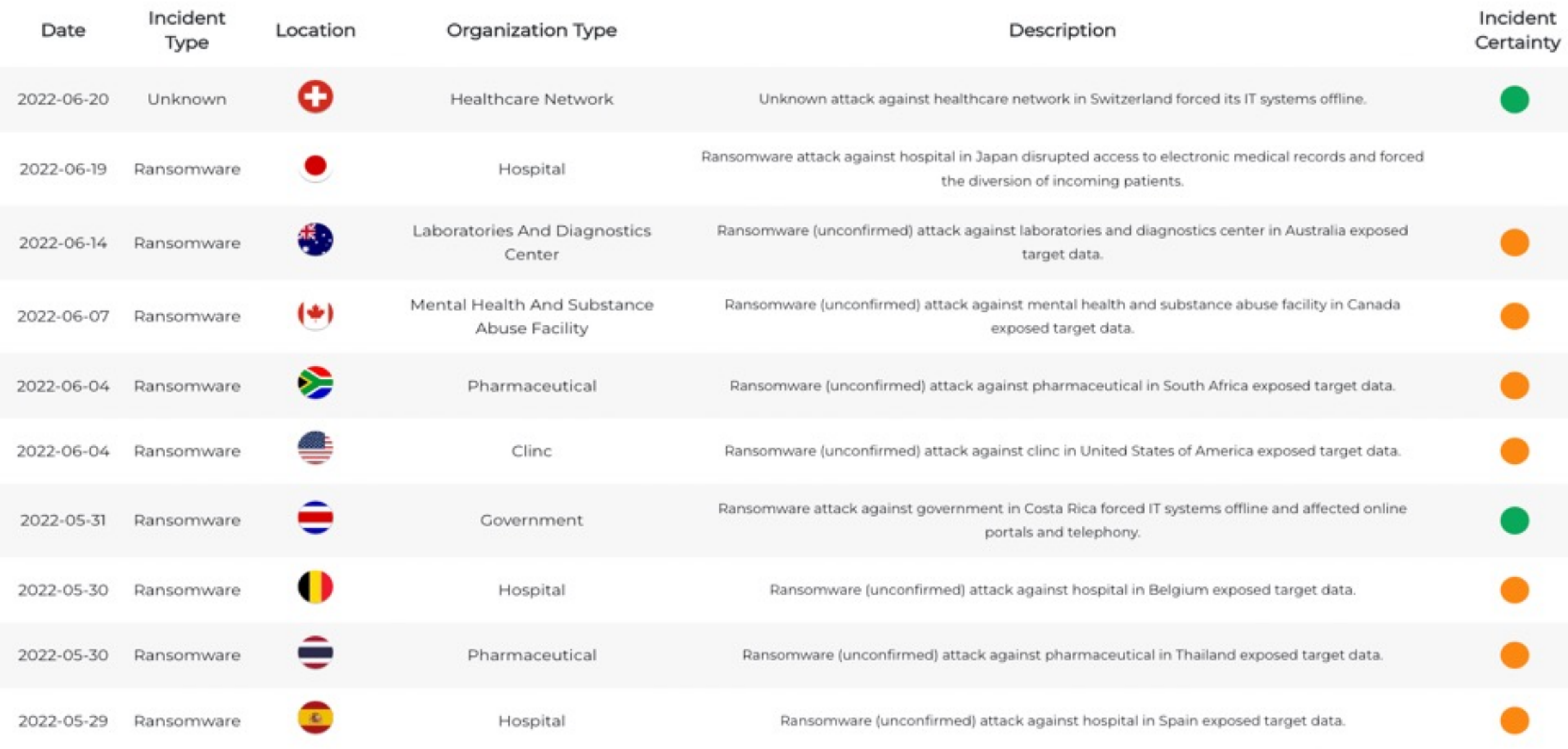
Incidents by top 10 ransomware operators over time (by month)



Ransomware operator's alleged involvement in incidents color-coded by sub-Sector

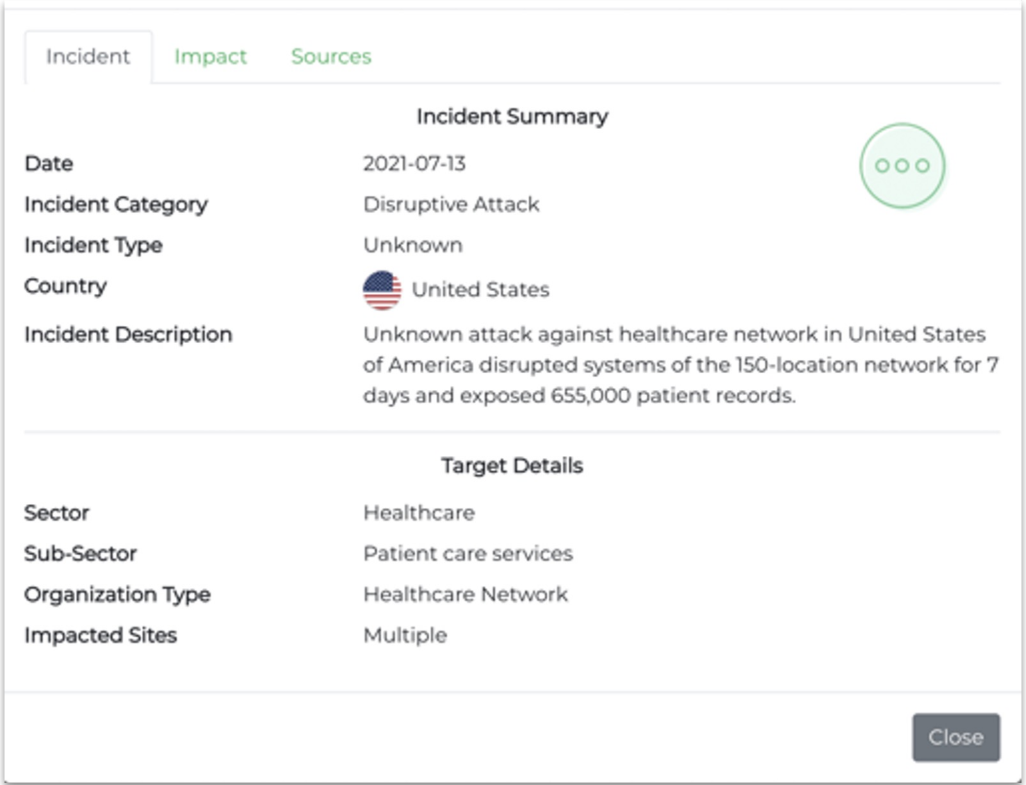


Incidents Table



Date	Incident Type	Location	Organization Type	Description	Incident Certainty
2022-06-20	Unknown	🇨🇭	Healthcare Network	Unknown attack against healthcare network in Switzerland forced its IT systems offline.	🟢
2022-06-19	Ransomware	🇯🇵	Hospital	Ransomware attack against hospital in Japan disrupted access to electronic medical records and forced the diversion of incoming patients.	
2022-06-14	Ransomware	🇦🇺	Laboratories And Diagnostics Center	Ransomware (unconfirmed) attack against laboratories and diagnostics center in Australia exposed target data.	🟠
2022-06-07	Ransomware	🇨🇦	Mental Health And Substance Abuse Facility	Ransomware (unconfirmed) attack against mental health and substance abuse facility in Canada exposed target data.	🟠
2022-06-04	Ransomware	🇿🇦	Pharmaceutical	Ransomware (unconfirmed) attack against pharmaceutical in South Africa exposed target data.	🟠
2022-06-04	Ransomware	🇺🇸	Clinc	Ransomware (unconfirmed) attack against clinc in United States of America exposed target data.	🟠
2022-05-31	Ransomware	🇨🇷	Government	Ransomware attack against government in Costa Rica forced IT systems offline and affected online portals and telephony.	🟢
2022-05-30	Ransomware	🇧🇪	Hospital	Ransomware (unconfirmed) attack against hospital in Belgium exposed target data.	🟠
2022-05-30	Ransomware	🇹🇭	Pharmaceutical	Ransomware (unconfirmed) attack against pharmaceutical in Thailand exposed target data.	🟠
2022-05-29	Ransomware	🇪🇸	Hospital	Ransomware (unconfirmed) attack against hospital in Spain exposed target data.	🟠

Incident Details

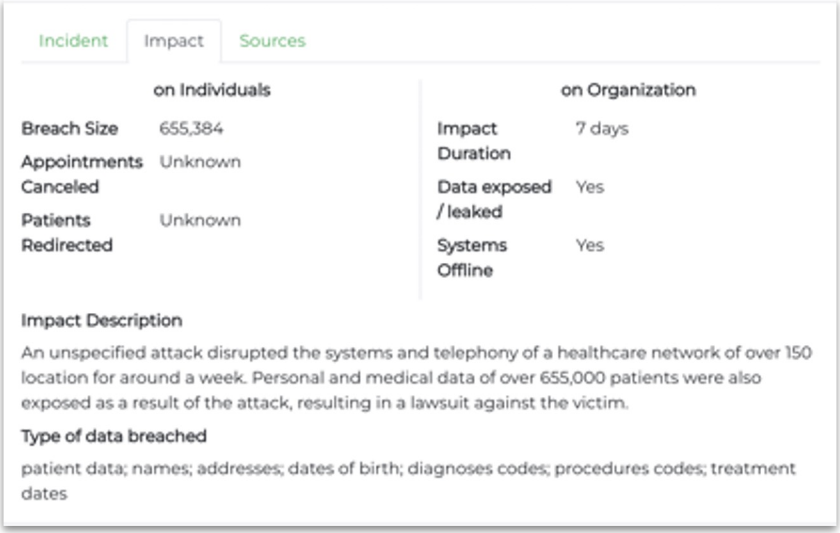


Incident Summary

Date	2021-07-13
Incident Category	Disruptive Attack
Incident Type	Unknown
Country	United States
Incident Description	Unknown attack against healthcare network in United States of America disrupted systems of the 150-location network for 7 days and exposed 655,000 patient records.

Target Details

Sector	Healthcare
Sub-Sector	Patient care services
Organization Type	Healthcare Network
Impacted Sites	Multiple



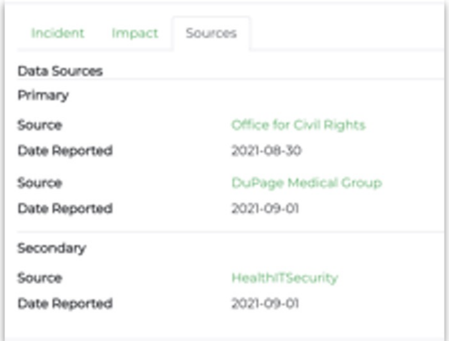
on Individuals		on Organization	
Breach Size	655,384	Impact Duration	7 days
Appointments Canceled	Unknown	Data exposed / leaked	Yes
Patients Redirected	Unknown	Systems Offline	Yes

Impact Description

An unspecified attack disrupted the systems and telephony of a healthcare network of over 150 location for around a week. Personal and medical data of over 655,000 patients were also exposed as a result of the attack, resulting in a lawsuit against the victim.

Type of data breached

patient data; names; addresses; dates of birth; diagnoses codes; procedures codes; treatment dates



Data Sources

Primary

Source	Office for Civil Rights
Date Reported	2021-08-30
Source	DuPage Medical Group
Date Reported	2021-09-01

Secondary

Source	HealthITSecurity
Date Reported	2021-09-01

24 months analysis – key takeaways

Ransomware remains Dominant Threat

Human-operated ransomware attacks remain the dominant disruptive threat to healthcare services, constituting **86% of documented attacks**.

Geographic Shift of Victims

Whereas the United States was disproportionately impacted by cyberattacks with 57.6% of all the documented pre-2022 healthcare cyberattacks, it has since accounted for 39.8% of the global total. In comparison, states in **Europe** accounted for 24% of healthcare cyberattacks pre-2022 and constituted 43.4% of attacks from January to May 2022.

Attacks on National Healthcare Systems

Costa Rica: The Hive ransomware operator is said to have affected services at over 1,200 hospitals and clinics with its attack on Costa Rica's national healthcare service on May 31. Earlier in the month, a Conti ransomware attack forced the Costa Rican government to declare a national emergency.

Italy: Around the same time, the website of Istituto Superiore di Sanità was hit as part of a broader DDoS campaign against Italian government organizations by the pro-Russian KillNet collective.

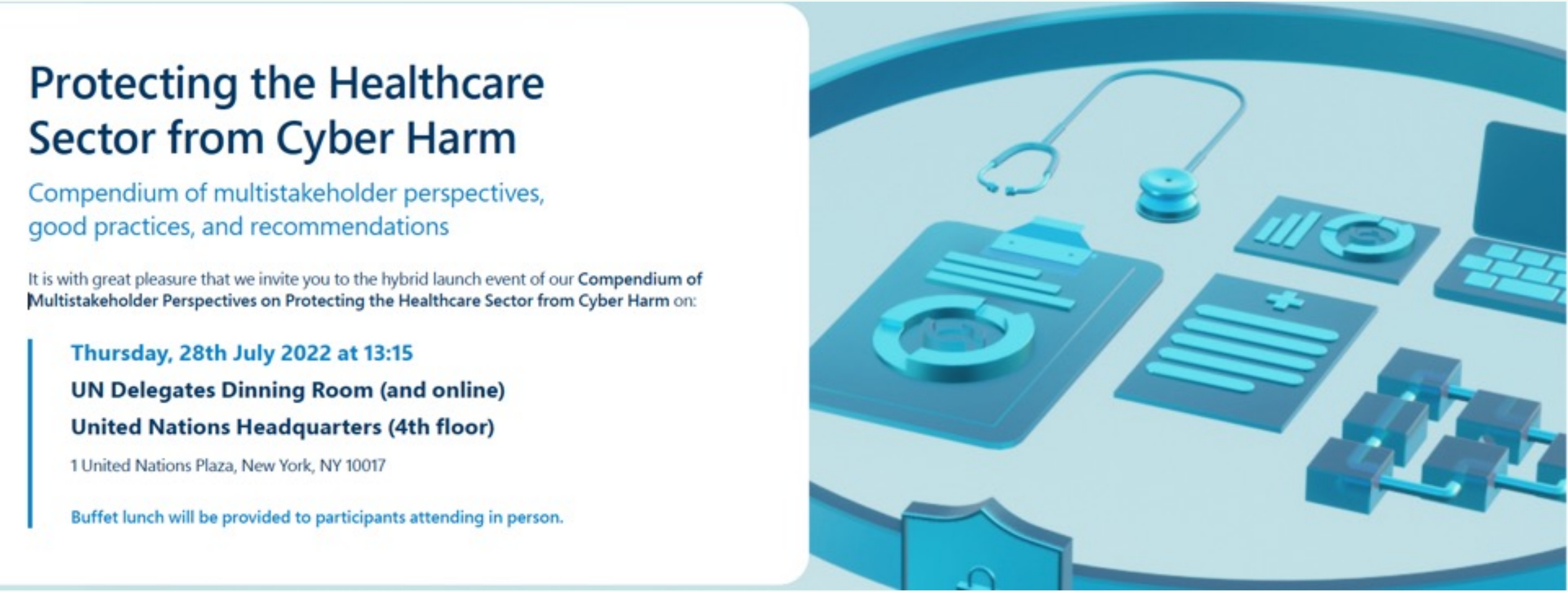
24 months analysis – What has Changed?

Pressure on Threat Actors: Early 2022 saw increased pressure on ransomware operators, including the arrest of alleged **REvil** members by Russian authorities and multi-country law enforcement efforts in late 2021.

Geopolitical Shock: The period preceding and the **Russian invasion of Ukraine** in February 2022 has seemingly led to a disruption to the Russian-speaking cybercriminal ecosystem, with both threat actors and perhaps their individual members flocking to take sides. This includes **Conti** – a dominant threat actor in the healthcare sector. An explanatory variable for the shift in targeting from a geographic and national healthcare network perspective may be due to their increased significance in the context of the war.

Changing Tactics: Several cybercriminal threat actors have shifted **from disruptive ransomware attacks to pure data theft extortion**. Prominent examples include CoomingProject, Lapsus$ and Karakurt – a now identified side-operation of Conti.

Upcoming: Compendium launch



Protecting the Healthcare Sector from Cyber Harm

Compendium of multistakeholder perspectives, good practices, and recommendations

It is with great pleasure that we invite you to the hybrid launch event of our **Compendium of Multistakeholder Perspectives on Protecting the Healthcare Sector from Cyber Harm** on:

Thursday, 28th July 2022 at 13:15

UN Delegates Dinning Room (and online)

United Nations Headquarters (4th floor)

1 United Nations Plaza, New York, NY 10017

Buffet lunch will be provided to participants attending in person.

Thank you

Francesca Bosco

fbosco@cyberpeaceinstitute.org

https://cyberpeaceinstitute.org

https://cpi.link/CITHealth