Indian Health Service

Change Healthcare - How One Cybersecurity Incident Caused Nationwide Impact to Healthcare

TYLER BRUMMER

CSIRT CSOC LEAD

08/13/2024

Change Healthcare Incident - Overview

Declaration of Major Cybersecurity Incident affecting Change Healthcare on Wednesday February 21st.

United Health Group (Parent company) SEC K-8 filing excerpt: "…identified a suspected nation-state associated cyber security threat actor had gained access to Change Healthcare information technology systems."

Early on details were not released if all servers and environments were brought down by Change as a risk control measure or if all services were impacted by ransomware.

Resulting impact to all major Change Healthcare services (https://solution-status.optum.com/), two core business functions impacted for IHS

- Pharmacy Claims
- Medical Claims

Incident held an Impact Severity Level II then escalated to III at HHS ASPR for impact to public health or safety.

Change Healthcare Incident - Overview

4TB of data stolen.

$22 million ransom paid by Change.

Actual incident cost estimates range around $2.4 Billion at this time.

Change CEO Andrew Witty testified to congress an estimated 1 in 3 Americans could be impacted by this data breach.

Initial Attack Vector determined to be a Citrix VPN application without Multi-Factor Authentication (MFA).

Change Healthcare Incident – Public Health Impact

94% of hospitals reported financial impacts

80% of hospitals said the attack affected cash flow

60% reported impact to revenue of more than $1 million per day

Difficulty for patients to access timely prescriptions

Interruptions to insurance verification

Change Healthcare Incident – IHS Impact Pharmacy Claims

Pharmacy Claims

- Change Healthcare Emdeon Pharmacy Switching solution – considered legacy, no timeline for restoration provided by vendor even a month after incident.
- Significant IHS impact, near-lowest priority by vendor.
- Situation necessitated migration to Optum eRxConnect HTTP Post Direct Internet Access solution
  - Migration would require development of new patch to be rolled out to hospital RPMS servers in an expedited beta-test.
- Early on (Incident+2weeks), technical bottlenecks apparent on vendor side, no correspondence or engagement from vendor other than generic “all hands are on deck”, “refer to the cyber response page”
- No clear guidance, expectations, timelines were available. Change Healthcare overwhelmed, downstream impact to all business partners.

Change Healthcare Incident – IHS Impact Medical Claims

Medical Claims

- Piecemeal – individually contracted services across multiple Areas.
- Two primary interfaces, Tyrula intermediary with Change Healthcare as a sub-contractor, or direct contracts with Change Healthcare.
- Tyrula scoped for 17 unique sites using Optum RPA service.
- 41 unique sites directly contracting with Change Healthcare with varying levels of 7 unique services:
  - Revenue Performance Advisor (RPA)
  - Direct Data Entry (DDE+)
  - Assurance
  - Clearance
  - AhiQA
  - Patient Statements
  - Payment Automation Accupost

Change Healthcare Incident – IHS Impact

General thoughts on impact

- No reasonable timelines were provided by vendor, only statements of priority and recommendations to move to Optum solutions that were not impacted such as iEDI (medical claims), or eRxConnect (Pharmacy POS/Switching).
- These recommendations did not take into account effort to transition services. Not simply a flip of a switch to resolve.
- ABSP patch development completed, tested, and rolled out by end of May restoring Pharmacy POS.

Change Healthcare Incident – Cybersecurity Technical Response

IHS CSIRT became aware of the Cybersecurity Incident the morning of Thursday February 22nd

CSIRT attended HHS Administration for Strategic Preparedness and Response (ASPR) coordination call for Change Healthcare incident.

CSIRT immediately ordered the shutdown of four LAN-to-LAN tunnel configurations which facilitated the secure connectivity between IHS Pharmacy services and Change Healthcare to control risk to IHS.

CSIRT and CSOC stood up a coordination bridge between security practitioners, network operations staff, ISSOs, and ISCs for two key focuses:

- Measuring business impact and pain points associated with the loss of this business partner.
- Investigating for lateral activity risk and verification of the severing of connectivity to Change Healthcare.

Tunnels were confirmed disabled, no lateral activity was found, and monitoring and network blocks were implemented to control risk based on traffic pattern finger printing if/when restoration was executed.

Change Healthcare Incident – Cybersecurity Technical Response

Threat intelligence - open source, or as collected by the FBI, CISA, HC3 or other partners in the space, was limited during the initial days of the incident.

Primary concern over a lack of quality threat intelligence. Concern if this was a novel attack vector to potentially action and mitigate any risk on the IHS side.

On 2/26-2/27 significant reports were coming out of a potential attack vector using ConnectWise ScreenConnect.

CSIRT implemented a data call for ConnectWise ScreenConnect and ultimately shut down the use of ScreenConnect on the IHS network via Endpoint Detection and Response and Next Generation Firewall blocks. Ultimately this was found to not be the initial Attack Vector for the Change Healthcare Incident.

Change Healthcare Incident – Cybersecurity Technical Response

On 2/28 ALPHV BlackCat Ransomware Gang posted on their leak site taking credit for the attack.

On 3/5 unverified news reports began circulating of Change Healthcare paying a $22 million dollar ransom.Change began restoring services one by one with focus on major provider pharmacies.

Change Healthcare Incident – Cybersecurity Non-Technical Response

CSIRT attended and provided twice-daily and later daily updates to ISC, ISSOs, and stakeholders to maintain broad spectrum communication and update channels.

CSIRT and CSOC maintained and operated a M-F 8AM-8PM coordination bridge to receive and respond expeditiously to requests for information, suspicious activity, or service impact reports.

CSIRT briefed the HHS Secretary Operations Center daily on cybersecurity and business continuity risks.

CSIRT attended and provided daily briefs to ASPR Change Healthcare incident coordination bridges.

Change Healthcare Incident – OODA Loops for Agility in Large-Scale Cybersecurity Incidents

Due to the sheer size and scope of the incident CSIRT operated an Observe Orient Decide Act (OODA) loops methodology. In the first days of the incident, new information would flow in every few minutes, in the next week, every hour, in the next week, every day, until eventually risk, severity, and paths to resolution were fully understood.

Each new source of information required an analysis, decision, and action and CSIRT maintained agile rapid response to developments during the incident.

Cybersecurity Incident Standard Response

Hour Zero –

Stand up coordination bridge between stakeholders

Interview to tease out risks/impact to IHS Mission if not fully understood. Never assume. These interviews lead to additional actions (OODA Loops).

Coordinate investigations into lateral activity.

Coordinate mitigating actions/controls/response actions to limit larger impact to IHS Mission as appropriate.

CSIRT acts as a hub for coordination between teams:

- Area ISCs, ISSOs
- Division of IT Operations
- Division of Information Security
- Leadership
- Privacy
- Disaster Recovery

Cybersecurity Incident Standard Response

Daily –

Provide daily updates to leadership and stakeholders.

Maintain coordination/communication bridge.

24x7 monitoring and support provided by Cybersecurity Operation Center.

Review for new threat intelligence and threat hunt as relevant and necessary.

Change Healthcare Incident – IHS Lessons Learned

1.) Large healthcare partner cybersecurity incidents can cause significant impact to the entire healthcare and public health sector.

- Per an American Hospital Association survey referencing >1000 hospitals:
  - More than 80% of hospitals said the cyberattack has affected their cash flow, and of those nearly 60% report that the impact to revenue is $1 million per day or more. In addition, the survey found that 74% of hospitals reported impacts to direct patient care as a result of the cyberattack. While hospitals are implementing workarounds to mitigate the patient impact and address the affected Change Healthcare systems, **most hospitals are reporting that these workarounds are very labor intensive and costly.**

2.) Preparation and planning for redundancy or backup services that can be enabled in events like these are critical for mitigation of impact for large scope cybersecurity events in the future.

- Services should be tested for agile activation and spin-up for continuity of operations in the event of catastrophic loss of service like was witnessed during the Change Healthcare Cybersecurity Incident.

Industry Lessons Learned - Planning

Continuity of Operations Plans.

Conduct Table Top Exercises (TTX) - Assume the worst/total loss of service, extended duration

Even if informal, highly valuable to help find major risks.

Standby contracts to fill gap/surge as needed?

Industry Lessons Learned - Technical

Multifactor authentication

- Huge efficacy
- Still has weaknesses at the user layer - MFA Fatigue, Social Engineering

CyberHygiene/Attack Surface Monitoring

Unrelated Best Practices

Have a plan

Have backups, both data AND configuration

Leverage publicly available cybersecurity resources:

https://405d.hhs.gov/resources

https://healthsectorcouncil.org/

https://csrc.nist.gov/publications/sp800

https://h-isac.org/

https://www.hhs.gov/about/agencies/asa/ocio/hc3/index.html

https://www.cisa.gov/stopransomware


INDIAN HEALTH SERVICE
PHS · 1955 ·