Are we ready for Systemic Threats in Europe?

Vasileios Mingos, Health-ISAC European Operations Director

In the beginning of 2024, the healthcare system in the United States experienced widespread outages and financial impacts following a cybersecurity incident at a large healthcare technology company. Change Healthcare is a provider of revenue and payment cycle management that connects payers, providers and patients within the U.S. healthcare system.

In February 2024, Change Healthcare was affected by a ransomware attack which prevented payouts to doctors on the platform. As a result, electronic payments and medical claims could not be processed leading to a widespread financial disruption. Worse yet, without visibility into insurance coverage, thousands of patient procedures were delayed and tens of thousands of individuals were unable to have their prescriptions filled.

Change Healthcare provides prescription processing services through Optum, which in turn supplies technology services for more than 67,000 pharmacies and care to more than 100 million individual customers. Change Healthcare processes 50% of all medical claims in the United States. The company is a leading technology provider of end-to-end revenue cycle management, clinical decision support and pharmacy benefit solutions, among other offerings. On its incident status page, Optum listed more than 100 Change Healthcare services that were affected. Among various other core functions being impacted were benefits verification, claims submission and status updates, remittance information transmittals and prior authorizations.

During the Change Healthcare incident, Health-ISAC played a key role as the authoritative voice for the entire healthcare sector globally. Within the first week of the Change Healthcare incident, Health-ISAC contributed to the response efforts in multiple ways. Health-ISAC provided a secure and trusted forum for members to collaborate, share information and learn from each other to protect their respective networks and maintain essential services. Health-ISAC also provided authoritative and responsible advice to the global healthcare community and served as a conduit for organizations to anonymously provide vital information that could be shared broadly.

Despite how damaging the attack and its aftermath have been, it is worth noting how the efforts of the healthcare community over the past several years have informed the private sector's response and helped mitigate a more catastrophic outcome.

Europe is no stranger to similar attacks. In May 2021, the Health Service Executive of Ireland suffered a major ransomware attack. The ransomware attack had significant impact on hospital appointments across the country. Several hospitals reported that they could not access electronic systems and had to rely solely on paper records. The COVID-19 testing referral system was also taken offline. In June 2024, Synnovis, an agency that manages labs for NHS trusts and general practitioners in south-east London, was the victim of a cyberattack. The attack had a massive impact as hundreds of appointments and procedures were postponed.

With all that in mind and the known differences between the U.S. and European healthcare systems, one has to wonder how ready European countries are for similar systemic threats. When services

converge to a great extent, and human health and well-being is at stake, the general population wants to feel confident that the disruption of those services will not impact them. Are European countries in a position to protect against such threats? Has there been enough preparation for similar events, such as tabletop exercises? Has the convergence of services been documented and accounted for?

To avoid negative impact Health-ISAC suggests:

1. Identify and analyze health sector systemic risks
2. Determine key supplier and sector concentration risks
3. Discern lessons learned and update Incident Response Plans
4. Hold industry exercises to identify single points of failure and communication gaps

The cyber threats that target the healthcare industry are the same around the globe. All of us have to be in a position to be informed about them and protect the industry against them. Public and private partnerships are important in this ever-expanding threat landscape.