Maryland Departments of Health and Information Technology Provide Additional Update on Network Security Incident Response

January 12, 2022

The Maryland Departments of Health and Information Technology today provided an additional update on the network security incident that was discovered on December 4, 2021.

Statement from Maryland Chief Information Security Officer Chip Stewart

“As you are aware, the Maryland Department of Health experienced a service disruption on December 4th as a result of a network security incident.

While the investigation is ongoing—and is occurring on a parallel track to our restoration efforts—we can confirm this much today: this was, in fact, a ransomware attack.

Ransomware is a type of malware that prevents authorized users from accessing data and systems until an extortion payment is made. We have paid no extortion demands, and my recommendation—after consulting with our vendors and state and federal law enforcement—continues to be that we do not pay any such demand.

At this time, we cannot speak to the motive or motives of the threat actor. That said, both law enforcement and cybersecurity authorities have observed that health and hospital systems are increasingly being targeted by malicious actors during the pandemic.

Unlike many organizations, which take days or weeks to contain security incidents, MDH was able to isolate and contain its systems within several hours of first detecting the incident. It is in part because of this swift response that we have not identified, to this point in our ongoing investigation, evidence of the unauthorized access to or acquisition of State data.

I want to walk you through how that swift containment occurred:

During the early morning hours of Saturday, December 4th, MDH’s network team identified a server that was not working properly. The network team immediately launched an investigation to determine the cause of the technical issues.

Through routine troubleshooting, they identified activities that they felt warranted escalation to the internal MDH IT Security team. Shortly after that, the network team alerted the MDH Chief Information Security Officer (CISO) that they suspected a ransomware attack.

I was notified shortly thereafter and activated the State’s cybersecurity incident response plan through the Maryland Security Operations Center (SOC). This action immediately triggered a notification to the State’s Cyber-Response Team, including the Maryland Department of Information Technology, the Maryland Department of Emergency Management, Maryland State Police, the Governor’s office of homeland security, and the Maryland National Guard.

Additionally, I notified both the Federal Bureau of Investigation and the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency. These notifications are part of our standard response and playbook for cybersecurity incidents.

Furthermore, I activated the State's cybersecurity insurance policy through the State Treasurer's office, bringing external forensic resources and advisory resources to help ensure that we are handling the incident in the best possible way. The companies and personnel provided by the insurance policy are widely regarded as the best in the industry. These actions brought all the resources needed to facilitate a comprehensive investigation and secure recovery.

At my direction and in accordance with our standard procedures for incident response, MDH took immediate containment action by isolating their sites on the network from one another, external parties, the Internet, and other State networks.

As a result of this containment approach, some services were rendered unavailable and some remain offline today. I want to be clear: this was our decision and a deliberate one, and it was the cautious and responsible thing to do for threat isolation and mitigation.

In cybersecurity incidents, there can be pressure to reconstitute services quickly … and sometimes too quickly. All too common are stories of organizations that had to restart recovery efforts because of this, sometimes more than twice. We are recovering with deliberate action to minimize the likelihood of reinfection. I cannot stress how important this point is—in order to protect the state's network and the citizens of the state of Maryland, we are proceeding carefully, methodically, and as expeditiously as possible, to restore data and services.

In addition, under Governor Hogan's leadership, the State of Maryland will continue adapting and hardening our IT infrastructure and defenses, in order to help protect the information that is in our care."

Statement From MDH Deputy Secretary Atif Chaudhry

"Good morning, my name is Atif Chaudhry. I'm the Maryland Department of Health's Deputy Secretary for Operations. I want to briefly discuss MDH's efforts to ensure business and service continuity in the aftermath of this attack.

MDH and the Department of Information Technology (DoIT) are working closely to address this incident and have implemented the FEMA Incident Command System, or ICS.

Under this ICS system, we formed a Unified Command Structure to address the incident. This permits MDH and DoIT to jointly collaborate to manage and address all incident-related matters. DoIT provides the technical expertise and is taking the lead on network security and IT system recovery efforts. MDH is focusing on business continuity and ensuring the Department is able to continue to provide services that are in-line with our mission to promote and improve the health and safety of all Marylanders.

Importantly, MDH business units have existing Continuity of Operations Plans – known as COOP plans. They provide a methodology and plan for programs to continue performing essential functions in the event of an emergency or interruption of services, such as this attack.

MDH's COOP plans were initiated and implemented in the hours immediately after the incident was first detected on Saturday, December 4th.

It's important to note that all of these COOP plans have been implemented, executed, and modified accordingly, when necessary. That last point is critical, in that an effective COOP plan and recovery effort cannot be static, it must be adjusted to meet the particulars of the incident you're facing.

Immediately following this attack, and in accordance with the Department's COOP plan, MDH started assessing the business functions that were impacted and began to prioritize them.

In this instance, we are using a tiered system that is focused on mission critical and life-safety business functions. This prioritization of the Department's affected functions has led to the development of a Critical Path for recovery and bringing systems back online.

MDH also immediately began implementing modified workflows for business processes across the Department in order to continue to provide services in accordance with existing and modified COOP plans, focusing on mission-critical and life-safety services. The units that are using alternative processes are working diligently to ensure that they can serve the public's most urgent needs right now and resume their standard level of full service at the earliest possible opportunity.

These solutions include Maryland's previous decision to migrate to Google Workspaces. This has permitted access to a full suite of tools online unaffected by the incident, and allows MDH to continue to collaborate and save and share critical files.

MDH has also ordered additional equipment to implement the Department's COOP plans and modified business processes. This includes ordering 2,400 laptops, with an additional 3,000 being ordered this week. Additionally, MDH also ordered mifi devices, printers, and wireless access points to ensure employees have the equipment to do their jobs and continue to provide services to the citizens of Maryland.

Without a doubt, one of the Department's mission-critical functions is the State's ongoing COVID-19 response, and on that aspect we have remained fully operational throughout this incident.

MDH has also ensured that the Department's Healthcare System has remained operational throughout this incident while maintaining standards of care.

We are also working with cybersecurity and systems specialists to support our efforts, and these independent teams have been working alongside us since the earliest days of the response.

We will continue to simultaneously execute our COOP plan and modify processes to perform MDH business functions while working with DoIT and the cybersecurity team we have assembled to complete the investigation and fully restore all systems."