TRACIE
HEALTHCARE EMERGENCY PREPAREDNESS INFORMATION GATEWAY

LESSONS LEARNED FROM THE MEDSTAR HEALTH SYSTEM OUTAGE:

An Interview with Craig DeAtley, PA-C

In the related ASPR TRACIE video "Cybersecurity and Healthcare Facilities," Craig DeAtley described the March 2016 cyberattack on the MedStar Health system, which comprises 10 hospitals, more than 250 outpatient centers, and more than 30,000 employees in Washington, DC, Maryland, and Virginia. In this interview with Dr. John Hick (ASPR TRACIE's Senior Editor), Craig expands upon certain points raised in the video, providing a more comprehensive overview of the incident, lessons learned, and the recovery process. He noted several challenges, including program integration and interconnectedness and newer staff needing to learn how to keep records using more traditional (i.e., not electronic) methods. Despite these challenges, Craig felt that the response worked well overall, as the hospital system had planned ahead, exercised regularly, and established solid working relationships with their information technology vendors.

(Originally published in 2016)

John Hick (JH)

Craig, you mentioned that over 370 programs were impacted by the ransomware. What were some of the most critical programs, and how did you overcome loss of access to the data?

Craig DeAtley (CD)

Overall, we grouped programs into one of four key categories:

1. Clinical (e.g., lab, radiological, medication orders);
2. Administrative (e.g., schedules for the operating rooms, for clinics, and staff; various forms, and phone directories);
3. Logistics (ordering and acknowledging receipt of routine items, including food and other materials [and related vendors]); and
4. Fiscal (to include paying staff, and accurately invoicing and paying vendors in a timely manner).

So many of these programs are integrated, and as they came back up, we realized we needed a very clear understanding of each program and how they are linked with others. We also had to prioritize the programs, as it is not a good idea to try to restore them all simultaneously. In some cases, one program with a higher restoration priority was integrated with another program with lower priority; we recognized the need to be very flexible and set aside extra staff time for back-up/lagtime record keeping.

While healthcare facility staff know which programs they use daily (and would prioritize), this varies by specialty and category. In the case of MedStar, we all learned to be patient together. At a systems and facility perspective, we all now have much clearer and keener insight as to the interoperability and integration of our programs then we had at the outset of the attack.

> *The integration and mutual respect are both important; so is trust from senior leadership.*

JH

How robust was the cybersecurity annex of MedStar's emergency operations plan?

CD

There are two components of MedStar: standalone facilities, and the entire system they belong to. In addition to being part of the corporate emergency operations plan, cybersecurity was also part of each facility's hazard vulnerability assessment, and both had recently been updated. Each facility had their own downtime procedure to fall back on, but this event reinforced the need to take a broader, more comprehensive look at cybersecurity and not just rely on 370 appendices (i.e., one for each program).

Lessons learned were two-fold. We are still in the process of after-action reporting and gleaning information from a number of approaches at the corporate and facility levels. For those facilities with a plan in place, we learned it could always be broader. Those who depended solely on downtime procedures realized the need for a broader approach.

Planners need to consider two primary audiences, as the layperson's understanding of the plan (and their related roles) will differ significantly from those with more technical expertise. A comprehensive plan would meet both of these needs and allow each person to pull out the section they need. MedStar will be reevaluating training to develop more creative ways to ensure that staff at all levels and specialties/assignments are as prepared as possible, and rely less on short, planned outages to ensure readiness.

JH

In our field, we know that IT professionals are not necessarily part of incident command, but they are critical to the response. Do you think healthcare systems know who to pull in when an attack occurs?

CD

This was a classic incident in which the IT professionals providing the technical expertise were critical in helping corporate and facility staff understand the scope of the problem, but were not necessarily in charge. Getting incident command to bring those disciplines together

ASPR TRACIE hosted a cybersecurity roundtable featuring: **Craig DeAtley** (Director of the Institute for Public Health Emergency Readiness at the MedStar Washington Hospital Center) speaking about consequence management following the MedStar Ransomware Attack; **Steve Curren**, Director of ASPR's Resilience Division speaking about the cyber task force and the federal healthcare perspective on cybersecurity and cyber hygiene; and ICF International's then-Senior Vice President of Commercial Cybersecurity, **Beth Musumeci** discussing the critical steps healthcare entities can take to prevent cyberattacks. The panel was moderated by **Dr. John Hick**.

> *We all learned to be patient together. At a systems and facility perspective, we all now have much clearer and keener insight as to the interoperability and integration of our programs than we had at the outset of the attack.*

isn't always easy, but we did that—we have traditionally done that. Out of happenstance, foresight, or good luck, this experience reinforced that while IT/Information Systems personnel were not in charge, they had to be at the table. Another key takeaway from the event was the need for those at the table to be able to take a highly technical field with its own jargon and make it understandable to everyone else who has a response role. The integration and mutual respect are both important; so is trust from senior leadership.

JH

Were any cybersecurity professionals on site? What was your relationship like before the event?

CD

There are staff you depend upon every day to keep the electronic system operational and react when problems are encountered. MedStar has staff at both the facility and corporate/ system levels. In events like this attack, the system's IT senior leadership worked closely with the vendors whose software was affected. Especially when we got into recovery mode, key vendors had a physical presence at corporate headquarters and local facilities to help the process along.

> *When you prepare with regularity, you come up with creative and time-proven solutions."*

JH

How did you communicate about the event—both internally with staff and externally with patients and the public?

CD

Part of any incident revolves around initial notifications and alerts and we've become dependent on electronic systems to accomplish this. To address the challenge associated with these systems being inoperable, MedStar implemented several strategies. Corporate leadership held teleconferences two or three times a day with all command staff and leadership from individual facilities. Facility public information officers (PIOs) were part of a workgroup that met on a daily basis and drove the messaging, but all messages were ultimately approved by senior corporate leadership (not leadership from local facilities). Facility staff had in-person

> *If there was one surprise, it was the rapidity with which we lost everything. The near immediacy and completeness of the loss was surprising. We were practiced at individual workarounds, but we had never prepared to lose everything.*

meetings with leadership once or twice a day to ensure information was being pushed out early and often. This was supplemented by patient rounding and hand-carried printed information.

To keep patients apprised of the computer repair process, healthcare providers increased daily rounding. Facility staff also printed simple update messages and placed them on patient's food trays. Staff also posted signs at facility entrances, acknowledging the problem without detailing it. These messages were meant to be reassuring without being overwhelming.

When communicating with the public (including the media), PIOs and others must take data security and privacy concerns (such as HIPAA), and public safety concerns into consideration. What you say to the public has to be tailored very carefully. Corporate MedStar staff carefully and selectively responded to information that was being released to the public through the media.

JH

In the video, you mentioned that some of the newer staff had a hard time using more traditional means of record keeping. How did you overcome that?

CD

A lot of credit goes to the mentorship of senior staff (those that had been there, seen this, done that) with helping newer staff adjust to using different tools to keep records. Their assistance was invaluable…they were willing to take care of their own responsibilities and help others. Pharmacists, nurses, respiratory therapists—staff from many departments stepped in to assist others. MedStar also used printed messages and instructions to supplement face-to-face meetings and messaging. Multiple strategies helped staff understand how MedStar was trying to help them work around the problems. In many cases, staff reported having a positive experience, noting that there was an avenue for them to quickly provide (often in-person) feedback through leadership to incident command.

JH

What surprised you most about the attack?

CD

There was no "aha" moment. We knew it could happen. It was part of our hazard vulnerability assessment, and we had discussed cybersecurity at meetings. If there was one surprise, it was the rapidity with which we

> *This wasn't a new experience for us. We've been working with the vendors for several years, so the relationship was solid. We also do system takedowns once if not twice a year for two to three days at a time. These do not impact daily operations, as we have backup systems that prevent the loss of any data. You need to have that tiered approach to team integration and solving the problem but you also need a tiered rehearsal of response to be successful.*

lost everything. The near immediacy and completeness of the loss was surprising. We were practiced at individual workarounds, but we had never really rehearsed losing everything, much less all at once. Another compelling new experience was the amount of patience everyone needed and displayed while restoring the programs to ensure they did not miss any details or programming.

JH

What are the top three takeaways you think are imperative for healthcare facilities to incorporate into their cyber preparedness efforts?

CD

1. Facilities need to know that it's going to happen and more than once. Make sure that you have a comprehensive plan that looks at all of the response issues associated with being locked out or someone getting into your system. The plan needs to address the messaging, logistics, and security implications of a total system outage. Furthermore, plans and roles will vary when facilities operate on their own versus as part of a corporate structure.
2. Rehearse this plan like you would any other. Note that exercising cyber plans may be more challenging than those for other hazards, as it has to be done at various levels within the facility, as well as within the system, if applicable. Rehearsing for one program at a time will not adequately prepare you. You need to exceed your comfort level to prepare for a problem this vast.

Recognize that the response to a cyberattack is going to be an intense, stressful, extended operation that requires a skillful incident management team capable of running 24/7 for a period of time. Leadership has to be multidisciplinary and multilevel, and will need to flex the plan to adjust to the nuances of each situation. Record keeping and clear, concise internal and external communication is critical to a solid response.

Recovery is a marathon. While MedStar is 99% back in service, some of the individual files that were locked may never be reopened. As is the case in cyberattacks, the system went down a whole lot faster than it's going to come back up.

Dr. Hick comments: We're grateful to Craig for sharing his experiences. EVERY healthcare facility and system is at risk of cyber events that may vary from a denial of service attack on a switchboard to a ransom-driven attack on an electronic health record. These attacks will cause systems failures without any warning, so line personnel must be able to move to downtime procedures right away. Furthermore, IT personnel will have to do a very rapid situation analysis to determine the specifics of the threat. This may require shutting down additional systems – and these decisions may have to be made very rapidly, so the authority needs to be determined before an event.

Also, while IT staff have the technical expertise, the overall incident decisions have to be part of an incident command process – implementing and modifying downtime procedures, communicating (when many modes of usual communication may be down), and prioritizing system restoration (as well as making decisions about any ransom!) has to be performed in addition to the technical aspects of getting the system running. As with any incident, an all-hazards approach is key to success.

Despite careful attention on the user end (not opening suspect files/links) and the system end, these type of attacks are nearly certain to continue and increase in sophistication. Having a plan to recognize and respond to these events is just as important to maintaining facility operations as any utility failure plan or disaster plan. As always, there is no substitute for having a back-up system that staff are familiar with and that works.

Craig DeAtley, PA-C, currently serves as the Director of the Institute for Public Health Emergency Readiness at the MedStar Washington Hospital Center and co-shares the responsibility for facilitating MedStar Health emergency management activity. John Hick, MD, serves as ASPR TRACIE's Lead Editor on detail from HHS/ASPR. He is an Emergency Physician and Deputy Chief EMS Medical Director at Hennepin County Medical Center in Minneapolis, MN, and a Professor of Emergency Medicine at the University of Minnesota.