ASPR TRACIE Webinar Transcript
Healthcare System Cybersecurity Response: Experiences and Considerations
March 18, 2021

PowerPoint Presentation: https://files.asprtracie.hhs.gov/documents/cybersecurity-response-experiences-and-considerations-webinar-final.pdf

Recording: https://register.gotowebinar.com/recording/2999617667872996111

Moderator: Greetings. On behalf of the US. Department of Health and Human Services, Office of the Assistant Secretary for Preparedness and Response, I'd like to welcome you to ASPR's Technical Resources, Assistance Center, and Information Exchange webinar titled, Healthcare System Cybersecurity Response: Experiences and Considerations. Before we begin, we have a few housekeeping items to note. The webinar is being recorded. To ensure a clear recording, everyone has been muted. However, we encourage you to ask questions throughout the webinar. If you have a question please type it into the questions section of the GoToWebinar console. During the Q and A portion of the webinar we will ask the questions we receive through the console. Questions we are unable to answer due to time constraints will be followed up directly via e-mail after the webinar. To help you see the presentation better, you can minimize the GoToWebinar console by clicking on the Orange arrow.

Today's PowerPoint presentation and speaker bios are provided in the handout section of the GoToWebinar console, and we will be posting along with the recording of this webinar within 24 hours on ASPR TRACIE. Next slide. The opinions expressed in this presentation and on the following slide by non-federal government employees are solely those of the presenter and not necessarily those of the US government. The accuracy or reliability of the information provided is the opinion of the individual organization or presenter represented. Next slide.

Shayne Brannman: Well, hi there, everyone. My name is Shayne Brannman, and I am the Director of ASPR TRACIE, and I want to welcome new and old friends to this webinar. I want to thank you for what you do daily to enhance the preparedness, response, and recovery activities of your healthcare entities and communities. Your role is vital to addressing the daily and arduous challenges being presented. So your willingness to spend the next 75 minutes with us to further advance your knowledge is noteworthy. I also want to convey my heartfelt thanks to our awesome lineup of panelists and moderator for this webinar. Your willingness to lend your precious time and share your subsets of expertise so others might benefit is commendable and generally appreciated. Lastly, many thanks to Audrey Mazurek and the entire ASPR TRACIE crew for coordinating this session.

For our new friends to ASPR TRACIE on the webinar today, this slide depicts the three domains of ASPR TRACIE: Technical Resources, Assistance Center, and Information Exchange. If you cannot find the resources you are looking for in ASPR TRACIE website, simply e-mail, call, or complete an online form and we'll respond to your inquiry. Next slide. This webinar is an extension of the ASPR TRACIE resource released last month titled Healthcare Systems Cybersecurity: Readiness & Response Considerations.

We would like to specifically thank our colleagues at Nebraska Medicine and MedStar Health for helping in the development of that document, and for sharing their experiences today. I also want to note that our moderator for today's session is Dr. John Hick, and he was integral in the development of this resource as well as the ASPR TRACIE team. Specifically, we want to note that Dr. Laura Wolf and her CIP partners along with a lot of our inter-agency partners and subject matter experts across the nation are vital in the review and helping enhance the final development of the document, and we want to thank them all for their participations and invaluable input to make this resource a reality. It is now my pleasure to introduce you to Dr. Laura Wolf who serves as the Director of the ASPR Division of Critical Infrastructure Protection who will now provide some brief remarks before we begin the presentation. Laura?

Laura Wolf: Thank you so much Shayne. Thanks for having me and for all the amazing work that you and your TRACIE team do to help the sector be resilient. As Shayne mentioned, I'm the Director of the Division of Critical Infrastructure Protection here at ASPR. My team works closely with government and private sector partners, particularly those in our sector coordinating council to identify, assess, and mitigate risks to the healthcare public health sector.

We think a lot about different threats and risks like natural disasters, supply chain challenges, and infectious diseases. But let me tell you, a majority of our time is spent on the ever evolving cyber threat landscape. So I'm sure so many of you on this webinar have experienced a cyber attack, that's probably why you're here, they are frequent and impact every aspect of the healthcare sector, from the smallest physician practice to nationwide healthcare systems. You may be impacted directly, or lose services provided by an external vendor, but unfortunately, one way or another, it's more likely than not that you will need the resources like the ones discussed today, and will need to have a plan for continuing patient care through a cyber incident.

So, as we all know, 2020 has been a tough year for the healthcare sector, with the incredible heroics that you've put forth to care for the nation through the COVID-19 pandemic. The pressures on you have been relentless. And unfortunately the bad actors in cyberspace have also been relentless, recognizing that the healthcare sector might be focused on the pandemic. And there may be some delay of patching of systems or fine tuning on the security of connections made by employees working from home. They have absolutely taken advantage of that.

I have to laugh whenever I say this number. But there was a 9851% increase in attacks on healthcare over the course of 2019 into 2020. Attacks increased throughout 2020, with a peak in the September and October timeframe, and over the course of 2020, over one million healthcare records were breached per month. So it really has been a difficult year for all of us. And what makes it particularly hard is as ransoms continue to be paid, we're unfortunately seeing more and more double extortion back in for a second dip on those who have previously paid. So, how do you stay on top of best practices, and how do you stay ahead of the game?

Well, first of all, webinars like this, and information provided on the TRACIE Resources page is critical to prepare for cyberattacks. But I do want to flag a resource that my team provides. In this slide deck, you'll see a link for our Critical Infrastructure Protection program. And if you click that right on our homepage, you'll find a colorful graphic for signing up for our communications

materials. We have a weekly cybersecurity bulletins where we share helpful information on both the technical side and for communicating threats to a non-technical population. We also have a bulletin we use during cyber incidents to share the latest information from the Federal government and our key private sector partners on the security side. So I encourage you or others from your organization to sign up for those mailing lists so you can have the latest and greatest information that we can share with you to keep yourselves protected.

So on my side, we will continue to work closely with our colleagues at DHS, FBI, the intelligence community, and HHS, to provide you with the best possible information and resources to protect yourselves. But I can't emphasize enough that the information on today's webinar will be crucial to your successful planning and response to cyber incidents. You need a tool kit that you understand that's ready to go when there is an incident. So with that, thank you again to TRACIE team, the experts on this webinar today who will walk you through the information you are going to use, unfortunately, probably sooner rather than later. And with that happy frame of mind, I'll turn it back over to Shayne so we can get started.

Shayne: Thanks so much, Laura, and thank you for your leadership on this front for so many years, and continuing to enhance everyone's preparedness and response posture in this field. It's now my pleasure to turn it over to ASPR TRACIE's Senior Editor, Dr. John Hick from Hennepin Health who will serve as the moderator for today's webinar. John? Let's get started.

John Hick: Thanks so much, Shayne, and welcome everybody. Next slide, please. Just to set the stage, and I think Laura did a great job at this. If you haven't had a cyber event at your healthcare facility, or within your system, you're an outlier. Fortunately, most of those are the things that we've experienced, denial of service attacks, diversion of paychecks, you know, things that don't actually take down major clinical systems, But at that point, unfortunately, the care of patients can become dramatically unsafe if the right procedures, the right policies, and trained staff are not ready to implement downtime procedures immediately.

Also, business practices can suffer greatly, and we need to make sure that we are not only ready to respond, but also to sequentially recover from an IT attack from a cyberattack. And I think that's something that you'll hear loud and clear during our presentations today. Cyberattacks, as Laura mentioned, are really identified as a top threat in healthcare system, HVAs, there's not a healthcare system out there that is not defending their system against multiple attacks every day. And we need to make sure that we're sharing best practices and lessons learned across healthcare, so we can help each other be more ready for these attacks when they do occur, because they are occurring, they're going to occur. And if there's one thing that TRACIE does best, it's bring the experts together who have experienced some of these things so that they can share information with you. That's a value for the future. Next slide, please.

Amongst the resources that TRACIE has, we have a cybersecurity topic collection. We devoted an Exchange issue a while back to cybersecurity and cyber hygiene, and there's an associated video available for your viewing. And then as Shayne mentioned, there's been a major project undertaken with MedStar Washington and Nebraska, which you'll see the results of their healthcare system cybersecurity readiness and response considerations. There's some amazing resources in there that

if you have not already looked at those documents, I would make sure to do so because every facility, every system can learn something from the materials that are in there.

Also at the ASPR level, Laura is part of the Critical Infrastructure Protection Program, actually head set up for ASPR, and then we have the Health and Public Health Sector Cybersecurity Coordination Center, and there's a Joint HPH or Public Health cybersecurity working group that's part of the Sector Coordinating Council, that's a required element, it's a public-private partnership that helps define cybersecurity standards of practice for healthcare.

So if you're interested in getting involved with that, or, as Laura mentioned, subscribing to their weekly updates, please do find more information at these links And with that, I'd like to move on to our speakers today, which is the reason you're all attending so. Next slide please. First, we have Craig DeAtley who is the Director for the Institute for Public Health Emergency Readiness at MedStar Washington Hospital Center. Craig, thanks again for your contributions to the cybersecurity documents as well as for taking the time to be here today.

Craig: Well, John, thank you, and the TRACIE team for giving me the opportunity to join with the group. As you and Laura have alluded to, all of us on this call today need to be wary of the possibility of being attacked in one form or another. And among those forms of attack more than ever before is to our ITIS infrastructure. I would submit that not only should that threat be on everyone's hazard vulnerability analysis, but it should be among the highest of our priority listings. Like any other chance to be successful in responding to an incident that's included in our EOP, I've found success in, beginning with having a planning committee, one that's multi-disciplinary in its composition, including clinical and non-clinical personnel, involving, where appropriate, external partners from our local community as well as the vendors that we might call upon to assist us during a response.

For those that are part of a larger healthcare system, having representation from the system on your local committee, and having your facility represented on the corporate committee can be a win-win situation for all concerned. Like any other committee to be successful, they need to have agendas, they need to make a commitment to meeting regularly. And yes, there is benefit to keeping notes, for sure. Next. Some other useful steps, I would submit, include doing the following: Spend some time learning from others who've already undergone a malware or a cyberattack. What happened to them, how did it happen, are there vulnerabilities that they identified, something that is a vulnerability for you and your organization? And one of their lessons that they learned could be useful to you, all have value.

The plan itself can't simply be a compendium of individual downtime practices, but needs to be comprehensive and address subjects such as alert notification, starting authorities, who will be on the incident management team, and how will that team be activated and where will that be situated? Other sections should include business continuity, business impact analysis, and of course, recovery. It's also going to be important, again, for those of us that are part of that larger healthcare system, to understand what's the role and responsibilities of the system towards the local facility versus what is the independence, if you will, the individual decision making, and policy setting that the facility itself can set. Understanding both is critically important to being successful.

Next, please. Another critical point: sometimes you'd be amazed how many ITIS applications you and your system, or you and your facility actually have. So it's important to get that complete list, ensure that as new ones are added, that they include a downtime and recovery procedure to be added to the plan, and as programs are deleted that they're stricken from the record. Also of importance to recognize, it's not just the EPICs and the Cerners that are important, but we also need to make sure we have downtime plans and recovery plans for our biomedical equipment, for our internet based phone system, and for other facility infrastructure control systems as well. And like any other part of our emergency operations plan, we want our ITIS planning to be kept in duplicate and accessible in several different forms.

It's also going to be important to understand how each application relates one to the other both within the plans that are unique to your system or your facility, but also in those situations where one or both are linked to external partners, such as the Healthcare Coalition. Keeping those plans current on your list is important, as well. And making sure that the updates and the patches that are pushed out by vendors and subject matter experts are done on a timely basis, is another important response step as well.

Next. Some other points include considering involving an external audit committee, getting an outside pair of eyes, if you will, with some subject matter expertise to assist both with the planning on the one hand, but response guidance on the other can be helpful if available to you. Establishing a priority in how you will go about restoring those individual applications will be important, because it's unlikely that you're going to be able to bring them all back at the same time. In fact it may be encouraged that you bring them back in parcels and not try and do it all at once for a number of reasons. And don't just focus on the clinical impact of the outage, but the impact on the gift shop, the cafeteria, parking, security, the human resources, payroll, they are important to be brought back in a timely fashion, a smart fashion, should be addressed. But so too should the revenue cycle impact that restoration will have as part of our planning as well.

Of course with any plan, the more we practice, the more likely we will be successful in implementing it and establishing where gaps need to be addressed. But in this particular case, unlike the MCI, for example, how can I go about practicing isn't without its own challenges as well. Chances are, your request to turn off the system for real won't be accepted for a number of different reasons. So what are some of the other alternatives? Well, some of us have found maximizing the planned downtime added just to optimize the education opportunities that that affords us has the benefit along with doing mini drills, where we create a scenario on paper with accompanying questions, and then have the individual units and offices have to answer those questions is another way of practicing for the real-world situation.

Next, please. Other important steps related now to response include having a clear problem reporting process, Who do I notify when I pick up on something being missed at my desktop as an example? Having clarity on key definitions of who has the authority to implement the plan and how do I escalate through a series of response procedures, needs to be clearly stated along with having a duplication of the alerting systems particularly if some of those alerting systems are dependent upon the very system that just has been taken down. And as you will hear, Dawn or someone else speak to later, have a go bag that contain some critical response items has a practical benefit, as well.

Next. Communication is going to be critical, but how best can I do it? Phones, runners, radios; there's answers, plan for what those answers should be. Recognize also that in this particular situation, it's more likely than not, this won't be over in an hour or two. So it will be important not only to have a strong leadership team at the beginning, but to be able to sustain leadership over 24/7 period of time. And look at that need for an extended commitment to having downtime subject matter expertise available to roam around the facility to address concerns at the local level, and even do just in time training is needed too, because many of us will go to a downtime procedure that includes written records in mass, having a plan that addresses how will they be secured, how will they be archived will be important; not just how will I go back and enter that data as part of my recovery steps.

Depending upon the nature of the outage and its extent, logical question to ask is, can we continue under these circumstances to still be able to provide high quality and safe patient care?
Chances are, you will, but you need to be monitoring that on a continuum, and recognize when you can't will be the time that you may have to call upon others and begin a transfer process of some percentage of your patient population. Also sharing the updated workarounds that become known as we continue to go through this downtime learning process will be important.
Everyone needs to be aware of the same pieces of information across all shifts, not just the shift that started at the outset of the incident.

Next, please. What about the Health Information Exchange that many of us are part of? How can we access that during an outage, can we use it, should be understood before the outage, not discovered during. And because there will be an impact that in certain areas will require more labor support on the one hand, and two, some people will not be able to work because they are so computer dependent. There will be benefits to figuring out how can I redeploy those staff, where do I redeploy them to is important to our planning and response process, and recognizing too perhaps it will be smart to send some people home to be able to use their intranet system and communicate information back. That has some value. That also has some additional security concerns that should be planned for too. And recognizing that it's not just an effect necessarily on our clinical care, are safety officers being aware and involved, are security officers being aware and involved in addressing their respective roles and responsibilities, and addressing the concerns that appear that they can fix will be important to address, along with recognizing that there will be different expertise in responding to this type of situation. So that just in time training really will be an ongoing need and not just a startup need in all probability.

Next. Finally, recovery; that needs to be planned for too. Planning for this type of situation is like any other from our recovery perspective we want to start as early as possible, and not wait to the end. To do so successfully is going to require some dedicated staff just focusing on the end and not the beginning and the middle, and that group, maybe it's smart to include vendors because of the subject matter expertise that they bring, along with the ability to bring in some additional labor, perhaps, as well. And implementing that restoration priority list according to plan will be important, but adapting too the problems with that plan need to be flexibly addressed for sure. And communication we all know is so vital to any type of response, this is no exception to that rule. And having lived through a malware situation, I can tell you that it's not just trying to keep up with the beginning in the middle that will be challenging, but it's the immense amount of work that we

were able to do despite the outage. Now, oftentimes it's going to have to be re-entered into the system. That data entry process can be tedious and tiring, and very labor intensive. So having that reserve pool available to assist at the end, and not just in the beginning, and the middle will be important.

Next. And finally there may be some data, there may be some applications that we just can't get back. More times than not, it's probably because we didn't know about them. We hadn't included them in our planning and our recovery process. Financial implications should be expected. So keep records from the outset of the response, and contact your insurance company early to make sure you're addressing all of the documentation expectations they have to optimize being reimbursed for what may be lost financially.

Public messaging, we all know is going to be important from beginning all the way through as well. But in this situation, we may be influenced by outside parties as to what we can say or when we can say it or how best to say it. It may not be just an internal decision by itself, but in the end when it's all said and done, it's going to come down to how effectively did we communicate, how effectively did we implement our plan and adjust our planning to the real-world situation we're confronting, and how strong and adaptable was that leadership to address the scene and the unforeseen alike. John, that's it. I'm going to come back to you.

John: Great, thanks so much Craig. Craig, you and I have little experience which is a nice way of saying that we're kind of old, and so we're used to using paper charts and holding x-ray films up to the ceiling light and doing things like that. But there's, you know, most of our employees that have zero experience with a non-digital work environment. So how do you help them to educate them to the tools and the techniques needed to make that pivot?

Craig: Great question. And I wish I could tell you that it's an easy one-step answer but it really isn't. Number one, we have to recognize that that real problem exists. And so we need to draw upon the expertise of those senior members of our facility, of our healthcare system, and have them as their subject matter experts, have them roving around and providing the guidance to those that don't have that familiarization. And second, as I mentioned earlier, I think that we have to take better advantage of our planned downtime. It shouldn't be just -- the steps shouldn't be just that we announce that so and so is going to be down between 2:00 and 4:00 in the morning, and just that's it. We should be looking at that as an educational opportunity and not just an operational inconvenience. I think those are the two best answers from the experience that I have gleaned personally and learned from talking with others. John?

John: Yeah, that's a great point, Craig. When we go down for a software update, a lot of times everything just freezes while we wait that out, and even if there's not an intent to go to full downtime procedures, that's a great time to pull the boxes out and pull the forms out and make sure that people are thinking about if this was going to last longer. And maybe it will, you know, what would we do, and how do we cope? Well, thanks so much, Craig. Next slide, please.

We're going to go now to Dawn Straub from Nebraska Medicine, who is the Executive Director for Nursing Professional Practice and Informatics who will share some of the University of

Nebraska's learnings regarding their malware attacks. So Dawn, thanks so much for being with us. And again, thank you for your contributions to our cyber portfolio.

Dawn: Well, thank you. I just want to say thank you to TRACIE for all the work they did in helping us compile this playbook and hope that all of you find the information helpful, at least some of it, that's the main goal, right. I'm going to bring you the operational perspective from Nebraska Medicine, and then my colleague, Lisa Bazis will bring you more of the IT perspective after this. As we're all aware, the emergency management cycle has the four sections of preparedness, response, recovery, and mitigation. My comments are going to follow the same and focus mostly on preparedness much the same way that Craig did. Next slide, please. So really one of the things that we all need to think about, is preparing the mindset. Our IT department and personnel had done a very good job, in sharing with all of us in this organization, our vulnerability and discuss the likelihood of a cyberattack for many years. And the phrase we use is it's not a question if it will happen, it's a question when. And so the entire organization needs to be prepared. Craig hit on this too, it's not just the clinical staff, it's everybody within the organization, And I'm here to tell you, and you probably already know this, it's still going to be shocking, a bit unbelievable that it's really happening. But patient safety is paramount when your systems are down, our reliance on technology is so foundational to our processes, our practice, our execution, everything. So cyber hygiene really is a patient safety goal for everybody in the organization.

Next slide, please. So in preparation also, rely on your HICS training. Make sure that you are aware of the resources, the structures, and the communication channels that your fixed infrastructure can bring to the organization. And then rely on the trainings that you've gone through. It will give you a small sense of comfort. Next slide, please. So the resources; all departments must have business continuity plans. And Craig talked about this as well. I think, maybe we can all share the fact that this is difficult. Everybody has very busy schedules. It's not necessarily a priority at the moment, I can do it tomorrow, and then the next tomorrow, and the next tomorrow, and the next tomorrow. But it needs to be done, and it needs to include every department having an understanding of what they would do, how they would continue their service if they were without technology. What would that mean? And it's not a won and done either, it needs to be developed, and then systematically reviewed. You need to develop tools for approval and updates. You can't have everybody being a cowboy and going out on their own in doing their own thing. Within departments, it needs to be systemic in a sense of cohesiveness and collaboration, and then drill, drill, drill.

Next slide, please. As Craig mentioned as well, we have used go bags in our organization, we have listed here for you some contents that are in there in what we should do with the contents of these go bags. They've proven helpful in other incidents when we need to use them. The main goal obviously is to have things immediately available for staff that are caring for patients. When the adrenaline, when it's high is not the time you want people to remember and think about all these separate things, just having them all together. You may also have inexperienced staff on when the incident begins. So for all these reasons, really think through what would be helpful in a go bag.

Next slide, please. In Forms, as Craig mentioned, we need forms, right, when we can't use our electronic health records. But forms are only as good as access to them, knowing how to use them and how to get the information to and from the right people. So store your forms in many locations

in many formats. Depending on what parts of your systems are down or inaccessible, you need to be able to get to these forms. And then again as emphasized earlier, many newly licensed staff don't know how to document in a paper roll. They need examples of completed forms. So with your forms, including example of how to complete it, and annotate on those examples about what the critical points are. And then you're still going to need staff at the elbow to assist. I may fall into the same category as Craig and John and I felt incredibly useful during this because I did grow up in a paper world, so I could help people learn how to document quickly with that.

And then know how to manage your workflows. So the medication orders, how are they going to get to pharmacy, lab specimen orders, how are they going to get to lab, how are you going to get results back. Think through all of these items in your business continuity, in moving the paper around, which we actually celebrate in not having to do. Next slide, please. So then if you happen to have an incident, you will implement. Rely on your training, rely on your structures, the adrenaline will be high, but pull everybody back into relying on your training. And I have just a snapshot of our structure that we have pulled together for HICS, and we definitely relied heavily on this. I'd also direct you to the handbook. There's a lot of very good practices listed there.

Next slide, please. And communicate, communicate, communicate. I think you're going to hear that so much that if there's one word you take away for these presentations, it will be that to all and often, but use your structure in your channels, do not overly rely on e-mail. We had a lot of people saying that they -- from every department that they needed to send information to the unit manager so they would know. But trust me, the unit managers are not sitting at their desk reading email. And they got bombarded, and so we needed to make sure that we reverted back to using our channels of communication, scheduling times of communication in coordinating and collaborating with what needed to be communicated when and to whom.

Informatics can also be incredibly helpful at this time, because they speak clinical, and they speak IT. And we found that incredibly helpful as well, thinking they all spoke the same language, but that is not always true. And then, as Craig said, you need to assign somebody specifically to manage your external communication in the media. Next slide, please. The workforce; this is really a time for all hands on deck. There are people who will not be able to continue to do their work, because they have no access to the systems they use. But we need to remember that we need a lot of extra help during this time. First and foremost is assign leaders with a cool and calm approach. This is a time of very high anxiety and you know who your leaders are that can lead through this. This is not a time to be worried about stepping on toes. Just assign those people who can manage through it, engage people calmly. Consider your deployment too, what we call [inaudible] [00:37:42] to the units. Not everybody descending upon units, but where the patient care is occurring you're going to need more help. We found people that we assign just as ones to be incredibly helpful; take this piece of paper over here, bring supplies from there to here, just all kinds of things that the clinical staff really needed to support.

Next slide, please. And then recovery. Again, communicate, communicate, communicate. This is when people really recognize the fact that this is a marathon and the incident is really far from over. When the system starts to come back up, what does up mean? It doesn't necessarily mean that it's ready for clinicians to start using, but you need to be very clear about that. And what data needs to be re-entered. Craig covered a lot of this, but I think the best analogy I heard was that

when the system went down, it was like flipping a light switch on. When the system comes up, it's like slowly moving a dimmer switch to get it back on. Next slide, please.

And, finally, mitigation. In mitigation, you need to be talking about the after action reports. And then we'll tell you that this was very difficult, because people are not even fully backed up and running and recovered from, from the incident, but it's very important to obtain. We capture what happened, what went well, what were the challenges and turn those into lessons learned to generate solutions for those challenges and reinforce best practices. Which in turn, you put back into policies, practices, in your preparation, and then disseminate the updated information, continue with those best practices and drill, drill, drill.

So that's all I have to share and I am going to turn it back over to John.

John: Dawn thanks so much. Just a question for you about how you made sure to integrate your IT into your HICS. We see that as kind of a common issue is that often IT is seen as taking the lead on cyber planning and actually, there's an awful lot of clinical planning that needs to go in and during your response, sometimes they wind up partitioned a little bit from the rest of the HICS structure. So, can you talk a little bit about how Nebraska Medicine made sure to integrate and maintain dialog between the two sectors?

Dawn: Sure. I would say that, probably, using our HICS structure, we have a very specific channel through our logistics section, and the logistics chiefs made sure that we knew what was going on with IT at all times. So, we would have specific report outs. It started out, I think every hour and then moved to finally, every, twice a day. But there would be a time when there was a specific update during those report outs from IT about what was going on and what we needed to do and what we needed not to do, like don't go try to access these systems.

And so, that really firm structure within the HICS for the IT department to have a specific report out, was critical.

John: Great, thank you, Dawn. Next slide, please, we'll stay in Nebraska here, and go over to Lisa Bazis, who is the Chief Information Security Officer for Nebraska Medicine. So, Lisa, thanks for your perspective from the IT side.

Lisa: Hi, and thank you, next slide. So, the key component, I think, that we all need to really realize is that cybersecurity is not just an IT issue. It is, as John said, it's a patient safety issue. It's a business logistical revenue issue, and it's also a reputation issue. But really, it all rolls up to the Board of Directors. If your Board of Directors do not take cybersecurity as a priority to understand how it affects all aspects of your organization, you're really going to just be climbing uphill battle. And it's going to be really difficult to get yourself through an incident like this when it does happen. Next slide.

Having that line of sight to the board of directors and having it from a top-down approach, really provides the trust to the IT and the cybersecurity, their vision, and then they have their accountability back to them, which then turns into empowerment.

If your technical teams are not empowered to make very, very quick, difficult decisions, at the flip of a switch, as Dawn referred to it, it's, you're going to have a very, very hard time recovering and dealing with the incident. At Nebraska Medicine, we're very, very fortunate that we're aligned all the way up to the top, and that we do have the empowerment to be able to make a decision, such as, shut off this fiber connection, shut off this data center section, shut off this segment.

We can contain and help to minimize the effects of an incident. And we're not second guess as to our decision because we have proven our accountability, and they trust us to make those decisions for the betterment of the organization. Next slide.

All of this goes into your digital resilience and how do you know what you can and cannot shut off. How do you know what you can and cannot contain at a moment's notice? You have to provide, you have to have a digital resilient network and a digital resilient culture inside your environment. Which means that you really need to understand, as Craig was talking about, you need to have your application portfolio understanding, but you also need to understand how those are intertwined and connect to each other. And then, how -- what order would things have to be brought up into, for the business, but also for the patient safety aspect of it, because certain systems might be a lower ranking. But yet, it's a life or death situation at the moment for that, for a patient. Next line.

And this really gets into, a lot of people talk about, you know, cybersecurity is confidential. Confidentiality, integrity, and availability. But I really like to look at it as a holistic situation where we have this environment that we're in, and in that environment it has people, it has process, and it has technology. And not one of those three can be independent. And then, on top of that environment, there is your data. We must provide the confidential integrity and availability to that data, but we must do it in a safe manner. And so, how do we prevent it from happening?

How do we detect it if it does happen, and how to respond from a holistic approach? Going back to the people, process, and technology. Next line.

So this is where business continuity really comes into play. Because as Dawn was saying before, we don't always have the people that know how to do things in paper form. Not all systems will go down, so you can't drill on everything, because it's always a different recipe of, well, our cloud systems are up, but our on premise systems are down, or vice versa. And so, it's very difficult to have the concrete, if this than that. It doesn't work that way.

You have to be very agile, and you have to be thinking ahead, and you have to be able to understand how you will try to function in one of these situations. Next page.

So how do you build business continuity in this unforeseen world and this recipe of -- that can be any variation of it. Again, going back to what Craig says, know your applications and your system inventory and interconnections. Know how they work together. Does it make sense to bring up system A, if it really needs system Z to function? Don't waste your time on it. If it doesn't work, if it doesn't make sense in that time, prioritize your efforts. We at Nebraska Medicine have what we call our Application Business Value Rating System, where we have worked with our system administrators and the business owners of those. Because IT cannot work in a silo.

We do not understand how the business uses that application. So the business owners and the technical owners fill out this survey system that we have that gives it a ranking and a rating. So we know critical infrastructure where that is, we know our EMR, we know our lab system. We know our interface system, we didn't have all of these rankings going down. So we have a kind of and I put it in quotes, kind of "order of recovery." But as what we have found in our situation, also is that we had a very small niche system that was down.

However, if this patient did not get that treatment at that time, it was -- it could have been deadly to that patient. So, we were able to, through our trust and accountability framework, with our chiefs and our chairs, we are able to reprioritize and understand because of that communication, and in those multiple lines of communication, going back and forth, that we're able to reprioritize on the fly and get other systems that normally in an event, would be have considered lower on the totem pole.

We have drills, drills, drills, drills, drills, inside of IT as Dawn was saying too, we have drills, drills, drills, drills, drills, outside of IT. But what was really interesting is, what I think one of the main drills that people forget about having is the drill of the chiefs and the chairs with the IT and the other business leaders to ensure that we're all speaking the same language, full lines of communication, and who will do what, when, where, and how.

And during our incident, we had multiple times a day check-ins with all of the chiefs, the chairs, everything, and they also helped to keep the calm of the masses, the people, because we weren't able to talk about things and what, how everything's going, because we're still uncovering what was going on. And so it really helped to bring that communication out.

So I really stress having those types of meetings, call a meeting quarterly with your IT leaders, your business leaders, your chiefs, your chairs, of all of your departments, so that you can talk about when this happens, this is what we're going to do, this is the expectation of all of your teams, this is what we need, feedback from you, and vice versa. Next slide.

But then how do you handle the fire, when the fire really does happen? We're trying really hard to try to put it into perspective for people that were non-technical as I explain the different aspects of what an incident in the cyber IT world really does mean. And so we decided to use the analogy of a fire.

Because when you build a home or a building or anything, you put in a lot of protection mechanisms from the start to try to prevent the fire from even starting. But then you still put in your detection systems, you still put in your carbon monoxide detectors, your fire sensors, your water sensors, you put in all of these sensors to try to find different types of events, because as it is, it's a recipe. Not every event is the same -- has the same format, has the same indicators.

But then you also put in things such as suppression, you have water, you have halon. You have fire extinguishers. You have all of these different mechanisms to suppress different types of incidences, because again one size does not fit all. And then not only that, then you also build in containments like fire doors, ways that you can block it off, so it doesn't destroy the entire

organization or house. And then how do you rebuild it? What comes first? How does all of that happen once you have the fire? Next slide.

So taking that into the digital journey, if you think about the way a user or a system interacts with everything on your, in your environment, you have a person -- that person connects to a device. That device connects to a network. That network connects to an application. That application resides on a server system and then it also has data and storage behind it.

And you need to think about the fire analogy around every single one of these bubbles along the journey to understand where you need to put your efforts, what you can do to try to make yourself more resilient, and what you can do to try to prevent and detect and contain an incident when it happens. Next slide.

This helps you to create your gap assessment, so that you can then have a strategic plan to understand what technology, what process and what people do you need to be able to make additionally resilient environment so that you can react to a cyber event when it does happen. Next slide.

Then that gap assessment, it goes back to the Board of Directors to help set the direction for your entire organization to continue you on the path of your digital resilience. And that's all the slides that I have.

John: Great, thanks so much Lisa. You mentioned the importance of limiting the damage and having trust sort of up and down that chain. So, if you're the provider or the IT person monitoring at five o'clock in the morning, and something starts going a little bit odd with the system. If there's not that trust and policy in place, you could stand to lose a lot more. Can you comment on just the importance of early recognition and that containment strategy you talked about with the fire?

Lisa: Yeah, so you're exactly right. If you have to go to, if you have an incident, you find an indicator compromise and you see that something is just not right. And your people that are monitoring the systems are not empowered enough to call up the management or in our case, they all have my personal cell phone number. And they're empowered to call me at any time and we make those decisions. If you had to go to committees, call a group of people together, discuss what you think is happening, all of those things, you're going to waste time. And there's that -- the average event sits in your system with -- slight indicators of compromise for up to weeks, weeks before they actually have it. When it does hit and the bomb goes off as what we put an analogy of it’s just spreading like wildfire. And so you have to be able to contain that, if you don't have that empowerment and that trust to say, “Stop it, do this now,” then it's going to just spread, and your recovery is going to be months and months and months, versus trying to get it into days.

John: Great. Thanks so much. Next slide, please. Going to move into our question and answer session now, so if you have questions for our panelists, please put them into your question panel on the right-hand side of your screen.

I'll start with a couple of questions. One, I was struck when talking with both Dawn and with Craig earlier on about the supplies that you guys ran into issues with right away, that weren't really

anticipated when your systems went down, especially as far as like forms and printing and things. Can you speak a little bit about that and some things that facilities might want to keep in mind?

Dawn: Sure. This is Dawn. I think a couple of things that were surprises, for some anyway were that things like our copiers worked, but our fax machines didn't. The network was down, and so we had no faxing, which was not something we could rely on as well. Another surprise area, I think would be our entrances and exits to the building. We have lots of areas badge access right and especially our infants and women sections of the hospital, none of those systems worked. And so you have to place people, and have people know what they're looking for and watching for at all of these areas.

So, when I said all hands on deck, those were some of the things that we assign. And it just continues to be surprising the things that don't work. Temperature control systems, may or may not work. So, we were lucky that it was in fall and the weather was not too extreme one way or the other, but you may need to evacuate patient care areas based on working temperature controls. So, it's really, like Lisa said, hard to think about every single thing, that it's pretty pervasive.

John: Great. Craig, any comments about that? I believe you made some toner runs.

Craig: Yeah, I was going to say I agree with all of the sentiment that Dawn expressed. I would just say that I don't know that we were surprised by what we needed, because we had done some rehearsals. I think what was challenging was sustaining the response.
You know, usually when we drill, even for MCIs, is it's a couple of hours and then we pat each other on the back, 'Job well done,' et cetera. But in this situation it can go on not for hours, but for days on end. Do I have enough toner? Do I have a printer, as Dawn just said, that will work, versus a fax machine. Sometimes, we just don't fully appreciate how much of our operations on a daily basis, outside of patient care, not just patient care, is computer controlled.

And so, having that big picture, number one, number two, understanding, "Okay, this is what we're going to do to start, and this is what we're going to do to sustain," those to me, I think are some of the most important lessons for all of us to keep in mind.

John: Great, thanks Craig. We will stay with you for the first response here and then go to Lisa. Can you talk a little bit about, there was a dimmer switch phenomenon of coming back online that Dawn spoke of. And, I know this was an issue that you talked about, it's just the competing priorities as you bring systems back up, like, "Okay, this is easy system bring back up, but it's not the most important system. So, you know, everyone thinks their system is important, of course." So, can you speak a little bit about, you know, how you had some priorities going into the event, and also how you adjusted those during the event?

Lisa: Yep, absolutely. So, like I said, we do have an application business value rating system already in place. And so we have what we call kind of the framework for what we know we should work on first. And, but with that said, that's where we brought in our conversations multiple times a day, with the business leaders, and the chiefs and chairs of all of the departments, so that we could understand why it's most important to them on the front lines. Because maybe our e-mail system was not effective, but just, for instance, maybe e-mail isn't really the most important thing

to the organization right now, even though it's one of the applications that every single one of our users use. So just because every user uses it doesn't mean that it's actually the most important to the business continuity and bringing the people back up. So it's just really important to have those conversations, and then what also we noticed was in those chiefs and chairs meetings with the business units every, you are right, everybody's system is the most important.

But what it allowed, was it allowed for open lines of communication between the chief, to have them say, "You know what, I know your system is important, but this one, right now, because it's a patient safety issue or it's or it's something else, this is why we believe this is the right one." And then there was those conversations between those people that then dictated to IT, what to do. And it was great to have it, from their peers, from those clinical leaders perspectives, because then it was their decision. They were helping to drive this train, not an IT decision.

John: Great, thanks. And Lisa, another question for you, from one of our viewers. What training or certifications for IT cyber protection do you recommend personnel have?

Lisa: Well, this is -- there are so many out there today. There's clearly the generic cybersecurity competency exam such as security plus, CISSP, those types of things. But, so, I recommend that all of my staff work towards those. And then, I also have staff that are very more into -- some into network security, some into security operations, some into user security. So we kind of have a multi-faceted cybersecurity program where we have security operations, security engineering, identity and access control, and then governance, risk, and compliance.

And so each one of those kind of has their own flavor per se. So I don't really know besides the CISSP or Security Plus which one is like comprehensive over all of those, because those really touch on all of those. I don't know if I answered the question. I'm sorry.

John: No, that's helpful. So thank you. Craig, can you talk a little bit about how do you get to your business and clinical leaders, and then I'll ask the folks from Nebraska Medicine, the same thing, but it will start with you, Craig. How do you get your business and clinical leaders to buy into looking at business impact analyzes and then, you know, getting a good business continuity plan, organize once that's complete.

Craig: How much time do we have for the answer to this question?

John: It's easier after an event like that than before, right?

Craig: Yeah, absolutely. One, I think that a critical key is to, besides that committee approach that all of us have mentioned in one form or another in our presentation, I think also getting some key champions. Having your Chief Medical Officer, and your Chief Nursing Officer if not your President or CEO as on board, with your perspective of how important this issue is, than using them as both a sounding board, on the one hand for your ideas, but also to, to help sell your plan to others with the committee, is probably an important step to invest in doing.

Number two, I think you have to walk before you run, so don't try and eat the whole elephant at a time. Pick critical parcels of what you feel needs to be done, and work on those, if you will, show

some success in that effort, and that will also potentially help build a momentum as well as build, if you will, a process that has a chance in the end to be totally successful.

Those are two answers that I would start with. I'm going to let my colleagues perhaps to add on.

John: Lisa or Dawn.

Dawn: Yeah, I think it referred to the fact that we used or HICS structure very robustly. And, I think that it was glaringly apparent who had solid business continuity plans and who didn't when this happened. And fortunately or unfortunately a lot of health care providers are very competitive and our incident commander served as like a symphony conductor. And when there was a gap, basically just said go back and figure it out and come back to us with the solution.

And so it was sort of a public shaming, maybe, if you want to say in some ways, but also it was a collaboration of, if they don't have a plan we need a plan, call on whoever you need at this point in time. But then, as I mentioned, with their after actions reports we capture, all of that information and try to write it down so that we can put it back into preparedness for the next time.

John: Great, thank you. Whenever one of these events happens, there's always a tough balance between communicating with external partners, about the nature of the situation, but also not releasing more information that is necessary. So, Lisa, do you want to talk a little bit about how you guys balance the, your external facing communications there?

Lisa: Well I think that there is two facets of this, there is the external communications with the public and our PR team has an entire structure for how they communicate with people and they also have outside firms that they work with for how to communicate to the general. As far as inside healthcare IT, within Omaha where we are at, within the state of Nebraska and then with all of -- also within our region, I have worked really, really hard to have really strong, good working relationships with all the cybersecurity and IT leaders in the region.

And so we have formalized communication between us. We have escalation conversations, where we can reach out and say, if I send one of them a text and said, "You need to call me," they will call, we have these conversations. We all have NDAs signed between all of our organization. So we can help communicate and share indicators that compromise trustworthy, without knowing that it's not going to go out to the mass public, but it is to help with the safety of the entire region. So, I think that that is also very critical. If your region doesn't have those relationships, start building them now. Because I rely on them also to tell me, "Hey, we're seeing something here, and this is what it looks like," so that we can go and see proactively if we are seeing it also on ours. And we have, like I said, two-way communication constantly between all of the cyber leaders in the region.

John: Great. Thanks for that. We had a question about networked medical devices, as well as the risk that some Voice Over Internet Protocol phone systems may have as far as not only interruption in service to the system, but potential deletion of contacts, software assignment numbers. Did you guys face that at Nebraska, and then I'll ask, Craig, or do you have any thoughts on those issues since they, you know, unfortunately, a lot of things are linked to other things these days.

Lisa: From Nebraska's perspective, we're really not speaking on details such as that, but I do. I will tell you that it is something that everybody needs to really take a hard look at, their medical device, security program and how resilient is it and how up to -- how well is it being cared and fed. Because new vulnerabilities come out monthly. Is your biomedical engineering and clinical teams, are they patching the systems, are they protecting them, are they testing to make sure that when an incident does happen, what does that really mean? Because I think that that is one of the biggest gaps that most healthcare organizations have at this time.

Dawn: Yeah, and this is Dawn, I would just elaborate on that, that part of our thinking about business continuity includes things like, if you don't have an IV pump, if you don't have an electronic blood pressure and those kinds of things, what would you do?

So in our go bags, we had instructions on how to hang an IV to gravity encounters. Again, something that is just completely foreign to the younger practitioners. So again, it's back to business continuity and everything in putting that information where it's going to be needed.

John: Right, these days, it's like, "Why do we care if it's a 10 drops per mil or 60 drops per mil," right? And, Craig, any thoughts on communication system vulnerabilities, or medical device vulnerabilities from your standpoint? Oh, maybe Craig suffered a systems failure here. So, Craig are you still there?

Craig: I am there. I think my colleagues have answered your question. Well, I would simply add, then I think that one, you know, we know we have technology. We know, in turn, that we need to have some non-technological backups for when the technology goes down. And so, if it's a phone system failure, then we should have had in our phone system failure plan, what, what our options were. And so if it's tied to an overall cyberattack, then that's just one more plan that gets put into the mix to be activated by our incident management team. So my message is simply, plan on failure, one. Have redundancy to offset failure, number two.

John: Great. And Craig we'll stay with you for this next one, even prior to the incident you all have been quite proactive about, actually working with security consultants on, sort of, Tiger Team attacks on your system, and having pretty good relationships with information security consultants. Did you have any recommendations or any thoughts on the value of that and if there's a role to have, you know, retainers and work directly with those folks during an incident?

Craig: Yeah, as I tried to mention in my part of the presentation, some of us are blessed to be part of a larger health care system. And so both in the planning aspect on the one hand, and the response aspect on the other, we need to know, which is each other's imminent domain and how do we collaborate, if you were during the response to have joint decision making, et cetera, when it's most needed and most appropriate.

The second aspect, particularly from a health care system, management perspective is that, we probably will be more or well invested in subject matter expertise, not only inside the system and trying to bring them together through committees and the like, but also, knowing who our vendors are, and having subject matter expert outside of the vendor to try and give us the best advice.

And then the third element probably not mentioned enough today is that more and more facilities, if not everyone on this call, is going to have some sort of cybersecurity insurance. Now, and if that's the case, working with your insurance company, prospectively to understand, what is it that they can bring to the planning, what do they bring to the response, not just what do they bring to your recovery, is another important facet to being smart and ready.

John: Great, thanks, Craig. Lisa, Dawn any additional comments on use of consultants?

Lisa: No, I would like to second the cyber liability insurance carrier. They have so many resources available to organizations that we don't even realize are all there. And they also have an approved list of third parties that you can or cannot work with, that they already have arrangements with. So, if you are going to look at having a consultant or a third party assess you, it's in your best interest to look at that list first, and interview those people to determine which one would be the best fit for your organization, so that if you do have an incident, you don't need to start over with a different incident response firm. You can just continue the relationship with the firm that you already have.

I am a huge proponent of utilizing all resources that are available. So we use our cyber liability carrier often. They'll also come in and do presentations, they'll do training, they have tabletop exercise drills that they can help, and do for you also. So it's not just your IT or security teams trying to do that. And then, like I said, they have already fostered relationships with several of the firms that you would want to use anyway. And so using -- aligning with those firms and having a plan, even if you don't have a monitoring service by an outside firm, even if it's just a -- you have the legal forms and a retainer on hand, that will save you so much time when an incident actually happens, if you already have that going.

I've heard horror stories from some of my colleagues, where they didn't have any of that, certain plans, and so they couldn't even get the incident response tools into their network for six or seven days post the incident happening. So they sat there and not knowing, is it still spreading, is it still going on? So I really do recommend having all of those in alignment or knowing which ones you will engage when an incident does happen.

John: Great. Thanks so much. And our last question that we have time for today is, as I said, there's a question about where do you see the best place that information security, or, you know, issues like this report to in the chain for most impact and most attention. Does it come up through the finance and risk side, through the Chief Information Officer? How do we make sure that, you know, these threats get the maximum attention paid within the administrative chain of an organization?

Lisa: So that's an interesting question, because as everybody on this call, I guarantee you now has this silver bullet for how cybersecurity really reports through, through the organizational chart. At Nebraska Medicine, about, little over three years ago, they decided to pull cybersecurity out of IT, and so we are parallel with IT.

So my colleague, the CIO and I are partners. And we are strategically aligned in everything that we do, where, if he wants to bring in some new innovative technology, I am right there alongside

to make sure and put the guardrails up to make sure it's safe and secure. We have a great relationship, which again, has proven for the trust and accountability to the rest of the organization, so that we are empowered to make decisions. We report to the same person, who is one of the chiefs of the organization. So I think that we're also aligned very high in our organizational structure, which also sets the culture for the rest of the organization to know that we're not just a department. We have been working really, really hard over the last three to four years for the business to understand that IT is, and cybersecurity are not just cost centers that we are a strategic asset to the organization to bring, to move it forward.

And so it's really has elevated technology to the forefront at Nebraska, Madison. So, we're very fortunate again, because it does come from the top-down that we've been brought to those tables. As far as risk, I also feel like not only from a technology perspective with cyber putting the guardrails around technology to the rest of the organization, because of where we are aligned in our organization, I work very, very, very closely with the privacy, the legal and compliance teams. We meet multiple times a week, and this is all we talk about is the risks to the organization. Is it a people risk, a process risk, or a technology risk? And how do we help raise those to the higher levels, so that everybody understands. We have compliance readout meetings every other month where the larger risks do get brought up to the greater organization.

But I also have a clear line of communication to our Chancellor of the -- because we are an academic health system too. So we have our Chancellor and our CEO, I have a direct line to both of those. If a risk is imminent or a threat is imminent, and we need to elevate it immediately, we just do, because we have those lines of communication.

John: Great. It's outstanding to have that level of visibility and authority in the organization. So, and it served you well. So thanks to Lisa, to Dawn and to Craig for an outstanding webinar, and over to Audrey Mazurek for closing comments.

Audrey: Great, thank you so much, Dr. Hick and thank you again to all of our speakers. This is all the time we have for today. Again, this webinar recording and the answers to the questions that were submitted but were not able to be asked live today will be answered directly with you via e-mail. We will be sending out the link to the presentation and the recording of this webinar within 24 hours.

And on behalf of the ASPR TRACIE team, thank you so much for joining us today. Have a great day.

[End of audio]