

Are
You
Ready
for



the Digital

*For healthcare providers,
cybersecurity can literally be
a matter of life and death*

Darkness?

■ **Featuring Nassar Nizami, M.B.A.; Oren Guttman, M.D., M.B.A.; and Jonathan Gleason, M.D.**

“Everybody has a plan until they get punched in the mouth.” — Mike Tyson

In the late summer and early fall of 2020, healthcare systems were already months deep into the throes of the global COVID-19 pandemic. With the world turned upside down, hospitals were inundated with patients and constantly worrying about whether they had enough masks, beds, and ventilators. Health professionals put themselves in the line of fire to ensure the best care and safety possible for our patients.

But behind the scenes, a new—and very different—threat reared its head.

At this time of heightened activity, the FBI issued a series of warnings about cyber threats to health systems. No fewer than six large systems were attacked by ransomware. With 30 minutes' notice, they went digitally dark. In these ransomware attacks, hospitals experienced their entire digital environment going down at one time—internet, cellular, electronic health records, telemetry, and others. Jefferson Health realized that they had a plan for each component of the system going down, but did not have a plan for the entire system going down simultaneously.

A Close Call

Digital darkness, as it applies to health care, describes the severance of all digital activity—from telemetry and EMR to faxes and internet access—and it is an extremely dangerous situation.

So when Jefferson Health began to see unusual, accelerated behavior in several systems within their network, they recognized all the signs of an attack.

As Nassar Nizami, chief information and digital officer and executive vice president at Jefferson Health, explained during the presentation “Beyond Downtime Procedures — A Readiness Playbook for Total Digital Darkness” at AMGA’s 2022 Annual Conference, “We couldn’t discern any pattern, and in our minds, we were under a cybersecurity threat. That’s when we called all hands on deck.”

Upon investigation with fellow panelists Dr. Jonathan Gleason, the former chief clinical officer and executive vice president for Jefferson Health, and Dr. Oren Guttman, vice president for high reliability and patient safety, along with a number of operational colleagues and the information technology team, Jefferson Health determined the alert was a false positive.

“It turned out that a large amount of hours had made a change,” Nizami explained. “We were upset and relieved at the same time. But there was a period of five or six days in which we had all hands on deck.” After exhaling a collective sigh of relief, Jefferson Health took stock of their ability to respond to cyber threats.

Traditional concerns with cybersecurity pertain to enterprise and operational risk management, as well as the financial risks associated with cyber threats. While those

When we speak of the concept of “digital darkness,” we aren’t describing a single system going down.



concerns have not disappeared—the average cost of a breach is \$7.1 million¹—increasing precedence has been given to another area: patient safety.

Indeed, as Gleason described, “Modern health care has become socio-technical work. Almost everything that we do in the provision of care today happens in a digital world.” When that digital world is attacked, our patients are attacked.

When we speak of the concept of “digital darkness,” we aren’t describing a single system going down. Jefferson Health had planned EMR downtime procedures in place, for example. “We have processes that were put in place with some amount of expected failure rate that we’ve built back-up systems to discover and accommodate along the way,” Guttman said, “but we’ve never been able to plan for turning off the entire radiology system for a week. That’s never happened.”

As Guttman went on to explain, there are a number of concerns, ranging from increased mortality for patients with delays in diagnosis and treatment, to early warning and rescue system and mortality, to other clinical operational metrics like prolonged length of stay that would be significantly impacted by a digital darkness scenario.

Simulating Disaster

In short, Jefferson Health recognized that they were not ready for digital darkness. They immediately set out to create an *in-situ* simulation based Failure Modes Effects Analysis,² a previous analysis of simulated methods, that would stress test five critical emergency care processes:

- ▶ Acute MI
- ▶ Acute stroke
- ▶ Laboring female
- ▶ Trauma
- ▶ RRT and Code Blue

“We thought those were the places that if those things went offline, that’s going to be the greatest immediate threat to life,” Gleason said.

One of the first steps in preparing for the simulation was to look at the downtime procedures—to gather all the actual downtime materials Jefferson Health had—and to write down each question that arises for each step.

Guttman explained their human factors-based methodology. Every clinical values team was asked at every step of the care progression process:

1. How could this downtime step fail?
2. How would we know if this step is failing?
3. What would we do to recover if this step failed?
4. Could we contain failure if necessary?
5. If it is a critical task, is there redundancy built in?
6. What is the next step that happens in parallel? (Be granular.)
7. Is there a difference between what we think we will do and what we will actually likely do?
8. Are there any hazardous or “at risk” conditions or current workarounds in place that could quickly fail during downtime and become “fault” conditions?

A scribe captured not only the responses to these questions, but more importantly the new questions that arose.

“We’re actually looking into the abyss at this moment,” said Gleason. “What are the most important things we need to be able to do in order to deliver a baby? We’re talking about how to run all of these scenarios at once, and you start to tap into the complexity of this.”

Results

In-situ simulations for a total of five scenarios were tested. These simulations covered 12 units in one hospital, with 36 support staff members running the events, 10 involved in the trainings, and a total of 85–100 frontline staff participants. Altogether, the testing revealed 72 latent safety threats (see Table 1).

From these results, the team focused on some key areas.

1 Patient Identification: The area of patient identification is “challenging,” according to Guttman. “You’re going to need your admissions and discharge lists centralized and printed. You’re going to need to have a naming system for your trauma patients and all those patients who have not yet been moved from one environment to another identifiable.” This is particularly important to keep patients who have been admitted but are still sitting in the emergency room from falling completely off of the radar.

Table 1
Simulation Outcomes

Type of Threat	No. Latent Safety Threats
Patient Identification Issues	4
Communication Issues	6
Coordination Issues	9
Distinct Operational Software Failure Issues	7
Equipment Failure Issues	5
Distinct Clinical Operational Issues	37
Security Issues	4
Total	72

2 Communication: “There are all kinds of assumptions made about how groups communicate in a holistic, broad sense,” said Guttman. In a digital darkness scenario, those assumptions become an imminent threat to patient safety. “How will you get the code team to the bedside? What if there are dead spots in your hospital where people don’t hear things or cell phone dead spots?”

3 Coordination: Nearly all coordination processes have been digitized through call scheduling, day scheduling, fax machines, admission and discharge summaries, and much more. What considerations are there for vendor contacts and hospital policies and procedures?

4 Software: This may be the most obvious of all areas for disruption, but there are a number of software uses that may not immediately come to mind. “We ended up documenting 10 or more software programs that are used by radiologists in particular, and these things are suddenly in the workflows and processes of folks,” said Guttman. There were absolutely no downtime procedures in place for these processes. “We had to figure out how the folks would do the work and be able to care for patients acutely.”



Digital Darkness Stopgap List

- ▶ **Communication:** BCA computers with printed signage and log-ins (resident rooms); analogue phones, printed phone trees, fax machine number list, walkie-talkies with bandwidth for floors and units for emergency teams, vendor contacts list; printed hospital policies and procedures; care protocols; printed on-call lists
- ▶ **Equipment:** Back-up vital sign monitors packs, back-up off network pumps, extra printers, fax machines; external hard drives with large capacity
- ▶ **Clinical Orders:** Provider admission templates, preprinted order set templates by index admissions, printed nurse-driven protocols; printed flow sheets; printed diet orders and allergies, printed patient lists and printed MAR
- ▶ **Critical Safety Signage:** Allergies, dietary status (NPOs), code status
- ▶ **Staff:** Need many runners, an army of volunteers
- ▶ **Medications:** Lists of medications that require pharmacy verification; IV Drip rate tables
- ▶ **Labs Systems:** Preprinted lab labels with patient location and provider ordering the lab with cell phone
- ▶ **Radiology Systems:** External hard drives, high-capacity and quality jump drives
- ▶ **Nutrition:** Listed patient allergy info; diet orders
- ▶ **Environmental:** Manual thermometers for critical refrigeration (breast milk, implants, pharmacy, CSR)
- ▶ **PlanOpts/Security Concerns:** Color printer and photo system, high-risk area rounding protocol (ED, parking lots, mother/baby)

5 Clinical Orders: How many physicians know how to write a physical order or admit a patient to a hospital without Epic? Even if you remember being trained to do this physically, how many of your colleagues are even old enough to have been trained non-digitally? “Anyone who graduated after 2005 couldn’t do it,” said Gleason. And with so many nursing protocols built into Epic, acute or chronic heart failure patients are suddenly in unnecessary danger if there are no printed physical references.

6 Lab Systems: Labs are another potentially major source of hazard. Critical alerts from lab results require critical responses, and the geography of the healthcare setting may not be conducive to a fast relay of information. In these situations, Guttman said, “you need an army of runners to be able to do that immediately.”

7 Nutrition: Do you have access to necessary patient allergy information in a downtime scenario? What replacements are available for ordering systems?

8 Environmental: Think about the ability to control temperature. What drugs and substances need to be refrigerated, and how can you address that need if the systems are down indefinitely?

9 Security: There may be more security systems in place than you think about on a daily basis. Contingencies must be in place to maintain the security provided by badge entry systems, visitor management protocols, closed circuit cameras, supply room access, baby security (HUG system in the NICU), overhead paging, code silver, and panic buttons.

10 Equipment: Consider the sheer amount of equipment in a healthcare facility. Monitors, pumps, printers, anesthesia machines, Pyxis™ machines, anesthesia machines, IV pumps and servers, Xper cath labs—the list begins to feel endless.

But Guttman expanded on one piece of equipment in particular in order to illustrate the lethal threat of ransomware attacks: infusion pumps.

The Problem with Pumps

Ransomware has the ability to wreak havoc on infusion pumps. “The IT team could potentially say you need to turn off all your pumps now,” said Guttman, “because what some of these ransomware programs can do is tell you you’re giving 40cc a minute when you’re actually giving 80cc, or they could say you’re giving 40cc when you’re actually giving 20cc.” The medical implications are not difficult to imagine.

It’s not just a matter of being able to turn off the pumps, either. “You can only bring the pumps back online after validating that the pump is actually working,” explained Guttman, “because a lot of these malware can totally disrupt the internal processing of these pumps. You would in all likelihood also lose immediate access to all of the drug libraries and all their concentrations.”

“Imagine a scenario,” Guttman said, “where you have nurses who need to do drug validation and verification and have to go back to the nursing practices of years long ago, where they are literally counting drips of fluid from the specific tubing and looking at medication tables to understand the concentration of the medication, to determine how many drips per minute will give the correct amount of drug to the patient ... and then have to titrate those medications in real time by constantly counting drips and referencing medication infusion tables. Who even has those medication concentration drip charts available? Who has trained nurses how to use those charts?” How many hospitals have extra pumps on hand that could be deployed for immediate use? The majority of pumps today are on a single network to enable simultaneous updates to address patient safety concerns. In the end, Jefferson Health had to supply drip charts as a back-up mechanism to manage titration.

One more operational challenge warranted a more in-depth discussion: radiology services.

Radiology Risks

It is challenging enough for radiologists not only to lack access to prior studies in order to make comparisons, but also to actively work with images as they are received. There is highly specialized software for radiological use, and without the ability to transmit images centrally, a major gap forms.

“You would have to literally deploy a radiologist to every modality—one in CT, one in MRI, one in ultrasound—all these various places to be

able to see scout films off of the actual devices,” Guttman explained.


Even once these images are available, what can be done with them? Multiple external hard drives with large storage capacities would be required to store them, and then—once the systems are back online—take the time to upload the backup system to the main system.

And what about the X-rays that are taken all across the hospital? Either a radiologist must accompany the tech to read the X-rays in real time, or you will need a jump drive to port the images back to a central location. “The agility and the ability to do that in real time presents a clinical, operational challenge,” said Guttman.

A Stopgap Checklist

The panel closed by providing a high-level stopgap checklist. It did not intend this checklist (see “Digital Darkness Stopgap List”) as an exhaustive or holistic list, but rather as means of inspiring thought and considerations for your own organization.

Jefferson Health’s experience is not the end-all-be-all, and the specifics of your own systems will require slightly different approaches. As the panel stated, you should examine your own downtime procedures and run your own simulations so that you are prepared for when—not if—a cybersecurity breach threatens the safety of your healthcare delivery and the well-being of your patients.

Following this stopgap checklist, however, will set you well on the path to ensuring you can brave the darkness. 

Nassar Nizami, M.B.A., is chief information and digital officer and executive vice president. **Oren Guttman, M.D., M.B.A.**, is enterprise vice president for High Reliability and Patient Safety, and **Jonathan Gleason, M.D.**, is the former chief clinical officer and executive vice president at Jefferson Health.

References

1. H. Landi. 2020. Average Cost of Healthcare Data Breach Rises to \$7.1M, According to IBM Report. *Fierce Healthcare*, July 29, 2020. Accessed September 8, 2022 at [fiercehealthcare.com/tech/average-cost-healthcare-data-breach-rises-to-7-1m-according-to-ibm-report](https://www.fiercehealthcare.com/tech/average-cost-healthcare-data-breach-rises-to-7-1m-according-to-ibm-report).
2. S. Davis, W. Riley, A.P. Gurses, et al. 2008. Failure Modes and Effects Analysis Based on In Situ Simulations: A Methodology to Improve Understanding of Risks and Failures. In: *Advances in Patient Safety: New Directions and Alternative Approaches* (Vol. 3: Performance and Tools); eds. K. Henriksen, J.B. Battles, M.A. Keyes, et al. Rockville, MD; Agency for Healthcare Research and Quality (US). August 2008.