Weeks of lab turmoil follow cyberattack

Anne Paxton

April 2021—After he finished interviewing for a fellowship one morning last October at the University of Vermont Medical Center, pathology resident William O. Humphrey, MD, checked in to attend grand rounds virtually. Then the cyberattack struck.

It began mysteriously, with people dropping one by one off the Zoom screen and emails arriving only intermittently. Internet service grew patchy and a hospital staffer unmuted and canceled grand rounds, saying, "We aren't really sure what's going on."

From there, a cascade of failures indicated serious trouble. "All of a sudden we're realizing we can't sign into our EMR. We can't get into our email either. My phone isn't working on the Wi-Fi. Something is wrong," recalls Dr. Humphrey, a member of the CAP Informatics Committee. That was the prelude to a siege in which fax machines and penmanship were unretired from obsolescence, paperlessness became a relic of the past, and words like "runners" and "bouncers" entered routine laboratory vocabulary.

External agents had maliciously invaded and at least partially disabled the system. "It was certainly something abrupt. And our impression was that it may have been related to email phishing," Dr. Humphrey says, though no official word to hospital staff has clarified how it occurred and who engineered it and why.

Such attacks have become a serious risk for any enterprise reliant on IT, which in this decade is nearly all enterprises. But cyberattacks are special hazards for health care institutions. For the UVMMC laboratory, the effects of the attack ranged wide and continue to haunt operations.

As UVMMC realized hospital systems had been disrupted, a forced shutdown of the network was determined to be the safest recourse. "We went into downtime mode," says Christina M. Wojewoda, MD, associate professor and director of microbiology. Normally, that would mean an eight-hour break at most. "You get the critical results out verbally and everything else sits and waits for the system to come back. And then you work really hard to get all that work back into the computer."

But in this case, the backlog would continue to mount. Ahead lay weeks of downtime and chaos. "When you think about a cyberattack, you think about your electronic

Dr. Andrew Goodwin (from left), Dr. Christina Wojewoda, and Dr. William Humphrey at the University of Vermont Medical Center, where a cyberattack last fall sent the lab into prolonged downtime and chaos. “A cyberattack shuts down much more than you anticipated,” Dr. Goodwin says. [Photo: David Seaver]

health record going down,” says Andrew J. Goodwin, MD, division chief for laboratory medicine at UVMMC at the time and now vice chair for quality and clinical affairs. And it certainly did in this instance. “But your telephones are run by servers and software now. The fax machines are run by servers and software. Your pager system, your emergency alert system—everything lives on a computer drive somewhere. So a cyberattack shuts down much more than you anticipated.” In this attack, even the computer-driven pneumatic tube system at UVMMC went out of commission.

Four prior crises the lab experienced in recent years provided a telling point of reference as to the scale and severity of the cyberattack. “We suffered from a pretty significant flood,” Dr. Goodwin says. “Then our nursing colleagues went on a planned, 72-hour work stoppage. We had a go-live process to implement Beaker, our new Epic laboratory information system. Then there was COVID.”

The cyberattack was more stressful than any of those. The reason: “It was the cutting off of everything basic. It was not having a comprehensive playbook to draw upon. It was the inability to consult colleagues around the country for advice because, thankfully, very few labs had been attacked to this degree. And the uncertainty about how long it was going to last contributed to the heightened anxiety.”

“The hospital didn’t shut down. We still had patient care needs to meet,” Dr. Wojewoda says. But for nearly a month, all of the reporting requirements for routine testing, reference work, and SARS-CoV-2 results for the state health department were fulfilled manually.

Although some members of the IT department were put on furlough because there were no systems to work with, others were deployed to sweep all IT components and purge them of malware, Dr. Wojewoda says. “They had to go through every computer, scrub it, and make sure it was safe to use. In some instances new PCs had to be brought in.”

The shutdown of the hospital’s Epic EMR system meant masses of paper had to be deployed to report results. “Runners” helped the laboratory by hand-conveying results to floors and faxing and filing results. That was the assignment for Dr. Humphrey and other residents. “After we lost the network,” he says, “there was a rotating pool of all the residents and trainees in pathology, and some staff, who would make ourselves available to go to the room where we were storing the paper files, search for results, then physically take them back to the fax machine to be sent to the clinician.”

These tasks were an education in how much data results from a simple interaction like a primary care visit, Dr. Humphrey says. “We had three or four different areas of chemistry that each had its own filing system. We couldn’t just send the clinician the results, because then we would lose the only copy, so every result that had to go to a clinician had to be copied and then faxed.” Which was a challenge for a couple of residents in their late 20s. “I don’t think they had ever considered what a fax machine did until this happened.”

Without computers, test orders opened up further risks—although not as great as the risks that drug prescriptions posed to the UVMMC pharmacy, where an unclear entry could result in the wrong dose of a drug. “Pharmacy handwriting had to be very, very clean,” Dr. Wojewoda notes. Luckily for the handwriting-challenged, most orders to the laboratory involve checkboxes on a standard form.

Still, other measures were needed to head off problematic test orders at the pass. One of them was the purchase of a label-maker printer to avoid the syndrome of undecipherable handwriting. The laboratory also resorted to posting "bouncers" at its door. "We figured out as soon as the sample and requisition came to us, it was now our problem. So if all the information wasn't present that we needed, we would be stuck," Dr. Wojewoda says.

An added complication was that medical record numbers were usually not available—only a name and date of birth. But avoiding additional resolution time to fulfill test orders was a priority. "So the bouncers would review the requisition to say, 'Nope. You don't have the patient floor on here.' Or: 'We won't know whom to call if there's no physician filled out.'" And back the test order would go for completion.

At the same time, "We didn't want to broadcast what the problem was," Dr. Wojewoda adds. "The real idea of causing something like this is to incite panic, and the last thing you want to do, especially in a pandemic, is create more chaos." In fact, there was already a perception outside UVMMC that things might be out of control: The simple task of trying to tell external colleagues that staff would be off-grid for a while failed when the staff discovered those emails weren't going anywhere. "So it was just like we dropped off the map."

Dr. Humphrey, who was on his hematopathology rotation at the time, found that improvising solutions was the order of the day. "The clinics and the ORs were still going and we had to, on the fly, figure out how to do everything we would normally do for those patients without the technology that's pretty much required to function in health care now."

"All of a sudden we're wondering where the paper copies of all our forms are. Where's the binder with the printed-out procedures? How many copies of this result can we make? How can we shift what we do in the computer to, essentially, patient file folders and still keep the high quality of patient care we always pride ourselves on?"

Can a laboratory prepare adequately for the kind of disaster UVMMC experienced? "We were not ready for this. I will tell you that right now," Dr. Wojewoda says. Despite having well-established and regularly drilled downtime procedures, "we didn't have a procedure built for being down a month." In drills, "we could still perform testing and take care of patients. Because we used to do that without electronic medical records all the time."

"We create so much more information for patients now with different tests, imaging, physical exam findings, than we did back in the paper days. So we were trying to resurrect systems and thinking: Do we remember how to do this? And how do we keep it all straight? How do we get the treating clinician to understand what's important?"

First of two parts

Next month: cybersecurity

Electronic systems can flag results. "But it's much more difficult if everything's on paper. I've never seen more paper being used. It was unreal," she says. Because most of the laboratory's printers are networked, printing was unavailable. "People were printing things off at home and we were photocopying like there was no tomorrow because as soon as the results left the laboratory, we had no guarantee they would get to the person who needed it." Accustomed to ever-available electronic data, the clinical staff would take a result, walk away with it, and later call and ask for it again. "We kept having to make copies and resend the same result multiple times."

Having been through the experience, Dr. Wojewoda hopes to spread the word about the risks and the preparation needed to avoid the worst effects of a cyberattack. She'd like to see people "not get as blindsided as we did." Preparing for a longer downtime period than eight hours is a must, she says. Other tips:

- Have a process for shared samples.
- Design workup forms and report forms with all required elements and store printed copies on a shelf.
- Maintain hard copies of maintenance tasks.
- Outsource as much as possible because lower volume means fewer chances for error. Divert the outreach business.
- Buy as many laptops/tablets as possible and be able to plug them into printers.
- Think of all the people who will try to send email to you and send them a personal email address.
- Keep up to date a list of faculty/staff/resident phone numbers and personal emails.

For the microbiology laboratory at UVMMC, Dr. Wojewoda says the emergency preparedness plan now contains these and other additions:

- Have culture documentation worksheets printed and ready to use.
- Have paper result forms for each type of assay printed and ready to use.
- Keep a copy of the requisition with any testing logs and a copy of the result, filed in alphabetical order, for manual entry into the laboratory information system when systems are up.
- Create a spreadsheet for high-volume testing results to do a mail merge to print results, rather than handwrite results.
- Use label stickers to print plate labels for culture plates.

Rebuilding the EMR and LIS databases has been a challenge, UVMMC pathologists say. “We’re now trying to collate all of the worksheets we used and the ways we kept track of quality control and temperatures and all of the other regulatory requirements,” Dr. Wojewoda explains. “And there was considerable back-entry work to do.” For patients in the hospital at the time of the attack, “we had to get some level of information back in the system for them. So registration and nursing had to supply a bunch of documentation for those patients.”

Bits of information were often just stuck on paper forms in the laboratory, handwritten in most cases. “Sometimes some of the instruments would print out results,” Dr. Wojewoda says. “But we’d have to get it to inpatients, or outpatients across state lines, and then get all of those results back into the system afterward.” In microbiology, “we’re still working on that now in March of 2021.”

In all, UVMMC spent nearly four weeks operating without an EMR system—from Oct. 28, the date of the cyberattack, to Nov. 22 when the EMR went back online. Epic company representatives told UVMMC they hadn’t seen a cyberattack of this magnitude before. “They’d never had a customer down for so long,” Dr. Goodwin says.

It was not only the EMR, however, but also the hospital’s 300-plus other third-party applications that had to go through a recovery process before being reconnected. And the laboratory was hit hard by that. “To have literally everything turned off means that your communication methods, your interfaces with outside laboratories, your reference lab order interface—none of that worked,” Dr. Goodwin says. Mandatory state health reporting—augmented in 2020 by COVID-19 test reporting—was also disabled and had to continue by paper and fax.

For many of the laboratory's vendors, the cyberattack was novel and unsettling; it led them to temporarily sever their connection to UVMMC. "Some of our analytic systems, our analyzers in the lab, send data to and from the vendor on a regular basis. A lot of the vendors turned off all their connectivity with us because they didn't want to run the risk of being infected," Dr. Goodwin says.

"We couldn't even get some routine maintenance tasks done," Dr. Wojewoda adds. "We had to provide the vendors with proof that things were safe to get those instrument interfaces back up."

"It took us probably four to six more weeks," Dr. Goodwin says, "to get our essential third-party applications up and running. Overall, it took many weeks post-system reimplementation to mitigate the impacts" from the system shutdown.

Amid the system outage, a saving grace was the hospital's document control, a commercial system with no connectivity to the hospital. "As long as I could access the World Wide Web, I could go to our document control, which lived on a server with our vendor," Dr. Goodwin says. That allowed the laboratory to fill in one of the most critical missing pieces, the CLIA-required information on reference ranges and reflex testing, to allow providers to interpret an instrument printout that was their laboratory result. The links to this information were provided to ordering providers who could access important information via the mobile devices, so long as they were connected to a cellular signal, Dr. Goodwin says.

"There were no reflex testing rules anymore to use. We created a downtime manual for providers, updated daily, that had all the information they needed to know to do calculations, to understand reflex testing, and to understand reference ranges because we didn't have an EMR that could supply that information anymore." Providers could scan QR codes that the laboratory posted throughout the medical center and go right to the appropriate reference range table. "And we communicated very clearly that we could not provide a reference range on the result report."

Critical results posed yet more difficulties. Technical staff had to be sure to flag those results so the lab could call providers with critical laboratory results, Dr. Goodwin says. "So we prioritized what we thought had urgent, direct impact to patient care versus what is a regulatory requirement that is important, yes, but not as important as getting a critical result notification."

The biggest remaining impact on the laboratory is the need to deal with the welter of paper results—especially critical results like positive SARS-CoV-2 tests—in the wake of the cyberattack, Dr. Wojewoda says. "We have all of those results on paper that we're trying to get entered into the computer system while our staff are doing their normal jobs right now."

Unfortunately, as a rule, "what starts on paper stays on paper," she says. "It is too hard to go back and enter all the results when you bring your system back up." All SARS-CoV-2 results for patients who were in a bed at that point did get entered, and inpatient results are to be scanned into Epic with all the admission documentation. "But the laboratory is still deciding what to do with outpatient results."

"In planning sessions before turning the system back on," Dr. Goodwin says, "conflicting priorities arose, as the staff contemplated all the paper results in the 10 or 12 full-length, four-drawer file cabinets that are still in the conference room." The need to record the information electronically was complicated by the risks of adding those results so long after they were current. "We have chosen not to enter all of the results back into the EMR," he says. "It would take well over a year to do it, and weighing the cost against a potential transcription error or misunderstanding about the date of the result," the laboratory opted against it for select clinical laboratory results.

Anatomic pathology reports did get back-entered, with extra precautions to avoid confusion. "We had to really work with our Epic and IT analysts to configure the system, where we could, so that providers understood that back-entered results were not new tissue biopsies or a finding of a new cancer."

The lengthy crisis forced billing to take a back seat. “We didn’t send out any bills for weeks and weeks,” Dr. Goodwin says. The billing department determined which tests it was going to bill for and which ones it wouldn’t because the cost of manual billing probably would exceed the payback.

The financial setback is large. “Did the medical center lose money? Yes,” Dr. Goodwin says. “Our insurance coverage helped to offset some of the lost revenue and cost of the attack. But we are still incurring additional costs as the medical center restores our systems.”

The IT department performed heroically to recover from the cyberattack. “They had two shifts of our IT experts working flat-out to restore and rebuild the system’s servers—basically disinfect them of the virus and ensure the virus was no longer there—before they could turn the system back on. I think they were working from day one through go-live in 12-hour shifts,” Dr. Goodwin says.

But some other scars from the event will remain. When an institution is a victim of a cyberattack, “it puts you at higher risk for a subsequent virus,” Dr. Goodwin says. “So therefore all of the security has been turned up significantly on our systems,” meaning that many more steps may be required for pre-cyberattack processes.

In terms of the impact on patient care, a power outage would probably be worse than a cyberattack, Dr. Humphrey says. “The difference is that the answer would be clear: You need the power back on. As opposed to that long grinding frustration of so many unknowns, of not being sure what happened or what works.”

“Having the disruption from the pandemic kind of gave us practice at being able to function on unstable ground,” he says, and the IT department knew what needed to be done to recover and carried out the tasks methodically. “They seemed to have it down from day one.”

Despite the division between anatomic pathology and clinical pathology, Dr. Humphrey says, sharing cases is routine. “Tissue samples will turn into hematopathology cases and require flow cytometry, molecular, or even microbiology testing, and the EMR handles that interaction fluidly, can be called up instantly, and concisely reports on activity.” Being able to put all of that back together as normal communication was restored was the challenge. “Who needs to see what? What is still pending? What did these folks think about this case?” Those questions were not easily answered.

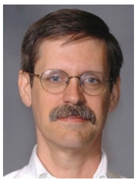
Looking back, “It was an interesting end to an interesting year,” Dr. Humphrey says. “In pathology we’re routine-based, and that systematic approach is what makes us good at avoiding mistakes. Then when people are thrown into chaos like that, it’s incredibly stressful.”

One thing that the crisis taught residents, he says, is that “our careers are going to be defined as much by our ability to avoid problems and threats like this” as by pathology expertise. “We are so tech-based and reliant on an integrated network that being able to keep those systems online is going to be just as important as that systematic approach that delivers great patient care.”

Attempts by outside agents to take over part of the operation of a machine for their own purposes, whether through malware in general or through ransomware specifically, are a continuing problem, says James H. Harrison Jr., MD, PhD, associate professor of pathology and director of clinical laboratory informatics at the University of Virginia Health System and chair of the CAP Informatics Committee. Like COVID-19, “ransomware could become one of the background viruses that infect systems every so often. You do have to put resources into defending against it. But we know more about it than we used to, and it’s now part of routine security operations.”

Instrument vendors may have external access to laboratory instruments, Dr. Harrison says, and they help the laboratory by collaborating on instrument management. “But that creates pathways into our protected networks and increases vulnerability.” Methods for securing these pathways exist, he says. “But the greatest threat has been and remains the ability to fool people into installing bad software on their own devices. That can work to subvert the protections.”

In the case of the UVMMC cyberattack, he says, “one question that would come up for me would be: Was that a failed ransomware attack, where the perpetrators realized it didn't go exactly the way they wanted?" For example, in such a scenario, the attackers may have bailed out after becoming concerned that if they contacted the target it would potentially lead to their getting caught.



Dr. Harrison

Tricks to fool people, such as phishing emails, robocalls that tell recipients to do something with their computer, or emails that make users click where they shouldn't, can be sophisticated and create vulnerabilities, Dr. Harrison notes. "If somebody fools you into clicking to install a piece of malware, the computer has no idea you're being fooled. It 'assumes' you know and want to install this software and so it's going to do it. And that, I think, is the most challenging continuing problem."

To keep vulnerabilities under control, laboratories should understand the havoc that can result if good practices are not followed. "We need to keep working to get the best security folks and best practices in place and follow those," Dr. Harrison says.

It doesn't take a ransomware attack to bring down a system, he adds, pointing to the Ochsner Health System's breakdown after Hurricane Katrina in 2005. "They had to shut down, and all their processes had to be done completely manually. That's why laboratories are required to have downtime procedures allowing operation of a system when the computer is temporarily unavailable." CAP checklist requirement GEN.73800 "Emergency Preparedness" calls for written policies and procedures that define the role and responsibilities of the lab in emergency preparedness for harmful or destructive events or disasters.

In addition to having downtime procedures, he says, laboratories need to practice them. "That's something a lot of places don't do. It is inconvenient and expensive and somewhat disruptive to the daily workflow, but it should be done maybe once a year, or at least periodically, so that you can make sure the downtime procedures are adequate and that people are familiar with them." The inconvenience is worth it, Dr. Harrison says, "because the alternative is really, really negative."

An understanding of informatics has become increasingly important in the cybersecurity battle, he says, and most pathologists, who are biological scientists at heart, don't naturally turn to informatics. Even teaching the basics of informatics in residency programs is challenging because it's difficult to define what a practicing pathologist needs to know, Dr. Harrison says.

"As a discipline, pathology has not achieved a common understanding of the importance and value of informatics. That's still being hashed out. At the moment, radiology is more informatics-oriented than pathology is." But that is likely to change soon, in his view. "Once whole-slide imaging becomes widespread, the default way of doing things, then pathology will be even more demanding in terms of data volume and processing requirements than radiology is."

However, it's already essential that pathologists and laboratories understand the importance of cybersecurity, recognize its value, have patience with the necessary requirements of best practices, and participate in ensuring they are adopted, he says.

Being a victim of a cyberattack is strong medicine, Dr. Humphrey says. "Cybersecurity matters, whether it's signing in from a personal device or opening emails you aren't sure about. All that will be ingrained in everyone who went through the experience. If we aren't careful about cybersecurity, we have to be cognizant that simple things can hurt us on a large scale."

Live and learn

In the wake of the cyberattack at the University of Vermont Medical Center, here is what the Department of Pathology and Laboratory Medicine is working on for emergency preparedness:

- Use of its online document control system (an external web-based system accessible by mobile phones, for example) as a way to post critical laboratory information, such as reference ranges, critical values, and reflex testing.
- A mechanism for communicating to all faculty, staff, residents, and the regional laboratories it serves when conventional communication methods such as email are unavailable.
- An approach to staffing, including recruiting volunteers, for all the manual processes needed to provide laboratory services.
- A workspace and infrastructure plan for manual paper filing, faxing, phone results.
- A process for using network laboratories (currently using different lab information systems), particularly for anatomic pathology. “We sent specimens, histology technicians, and pathologists to other labs in our health network to process and sign out cases,” Dr. Goodwin says.
- Ensuring active participation on the hospital crisis response teams/committees.
- A manual process (via paper or locally run computer spreadsheets) to track cases—essentially a manual pending log.
- Obtaining additional laptop computers including cellular connectivity.
- Obtaining secure USB memory sticks that allow for transfer and storage of data.
- Making routine rounds through the hospital to observe and learn where the laboratory can help with ordering and resulting.
- A system restart for the main LIS, interfaces, and third-party applications.
- A plan for billing/reconciliation.
- A process for reporting proficiency testing results when a lab has lost connectivity via web-based resulting.

Anne Paxton is a writer and attorney in Seattle.