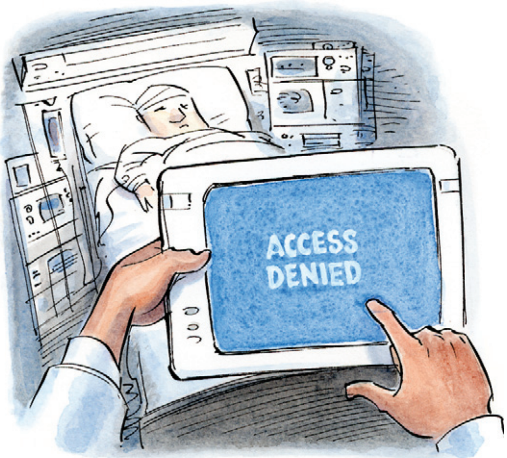
HBR Case Study

BY CAROLINE EISENMANN

COMMENTARY BY PER GULLESTRUP,
RICHARD L. NOLAN, AND
PETER R. STEPHENSON

When Hackers Turn to Blackmail

Lives are at stake when extortionists shut down a hospital's electronic medical records system.



UR NETWORK SECURITY SUCKS, the message read. *But we can help u. for 100K cash well insure your little hospital dont suffer any disasters.*

"Ridiculous," Paul Layman said to himself, deleting the e-mail. "The things people try to get away with on the internet!"

Paul, the CEO of Sunnylake Hospital, had been leisurely checking his inbox on a Friday afternoon when he found the illiterate e-mail from an unknown sender. He'd come to Sunnylake five years earlier with a vision of introducing cutting-edge technology to the small hospital. Paul was convinced that Sunnylake could grow only if it shook off outdated habits and procedures, and that switching from paper records to electronic medical records (EMRs) would improve the quality of care for the hospital's patients. After a careful search Paul had hired an earnest young man named Jacob Dale to be Sunnylake's director of IT, and the two had worked to execute his vision.

The success of the EMR initiative had transformed Sunnylake from a backwater community care center to a role model for small hospitals everywhere. The entire medical staff now used electronic readers to open patients' files. Many of the doctors had initially resisted the change, fearing that the new technology would divert attention from patients' signs and symptoms. As time passed, though, even the most devoted of the old school had been forced to admit that EMRs had increased efficiency – for example, by automatically checking for medication errors and drug interactions.

The shining success had turned Paul's fledgling IT department into a valued part of the hospital. The CEO considered EMRs to be his legacy – one that would serve the institution well for years to come.

The implied threat in the e-mail provoked no anxiety in Paul. He had great faith in Jacob, whose custom-tailored shirts and Vandyke beard belied his aggressive energy. While the system was under development, Paul had repeatedly insisted that patients' privacy was critical. Jacob had calmly and exhaustively explained that making records digital would also make them more secure. Nevertheless, Paul had been nervous when the system went live, but the past three years had quieted his doubts. Even though he knew that no computer system was perfect, he felt confident that the network was not in real danger – especially not from an

HBR's cases, which are fictional, present common managerial dilemmas and offer concrete solutions from experts.

Daniel Vasconcellos

extortionist who hadn't mastered basic typing skills.

He forgot about the matter over the weekend. But at 8:00 on Monday morning he received another e-mail from the same sender, with a subject line reading *We warned u.* The message field was blank.

The most difficult day of Paul Layman's career was about to begin.

Access Denied

"We've got a patient going into surgery!" the doctor barked. "I need those records now!"

The intern he was shouting at barely looked up from the device in her hands. She'd been there only a week, the doctor thought, and already she was proving her incompetence. He pulled the EMR reader away from her and impatiently entered his access code. The screen flashed *Access denied.*

> Sunnylake had no way of delivering records to doctors. The hospital was about to come to a standstill.

"What is this?" he growled. "I just looked at this patient's files yesterday!"

IT had designed the network so that records could be accessed only by the doctors, nurses, and administrators who needed them. Today, apparently, something had gone dreadfully wrong. The intern stood, arms akimbo, shaking her head. Resisting the urge to bang the device against a table, the doctor stormed down the hall to the IT department. He barely noticed the cluster of worried-looking nurses at their station, or the empty medication carts that should have been making their morning rounds.

At the heart of the department he happened on an unusual scene. A group of disgruntled doctors had gathered outside a glass-enclosed room in which several servers were humming on racks. Inside the room a few IT guys labored frantically. As the doctor drew nearer, he could see that each of his colleagues carried a device flashing the same message: *Access denied.*

Records for Ransom

Minutes later, Jacob was in Paul's office when the third e-mail arrived. In complete silence the two stared at Paul's computer screen. *We bet u want your stuff back. probly shud have protected it better. for the small price of 100K well make this go away.*

"What the hell is going on?" Paul demanded. "I've got doctors rioting in the halls."

"This is some kind of system-wide ransomware," Jacob muttered. "Instead of holding up a couple of people for 50 bucks a pop, these guys are holding up the whole organization. They want $100,000 for the decryption tool." His entire team was at work trying to restore the system. The programming that normally allowed only selective access to records had been altered to allow no access at all. Even the system administrators were shut out.

"How did they get into our system?"

"Maybe through an individual user's machine," Jacob replied. "Someone here might have thought he was downloading antivirus software – or updating an existing application."

"One idiot on our staff could have caused this entire mess?" Paul realized in a sickening instant that Sunnylake's IT department was simply not big enough or sophisticated enough to handle such a devastating problem. Over the past three years technology security had advanced significantly, but somehow Sunnylake had not kept up. Only days earlier Paul had been confident that the system was virtually impossible to infiltrate. Now he had to face the horrifying reality that it had been too weak all along.

Complete records were backed up on the network, so patient information wouldn't be utterly lost. But Sunnylake currently had no way of delivering those records to doctors who urgently needed them for patient care. The hospital was about to come to a standstill.

"This is –" Paul paused, at a loss for words. "Really bad. Really, really bad." He looked at Jacob.

The IT director's eyes had narrowed, and his expression was ferocious. "What kind of slime hacks a hospital?" he demanded of the screen. "Don't they care about hurting sick people? You think you've seen the worst, but these people get lower all the time."

"From what I've heard, hackers don't exactly subscribe to a moral code," Paul said, suppressing an urge to shout at Jacob. "They must have realized that our dependence on these records makes us particularly vulnerable. If you take down a normal site for a few hours, the company probably loses money. Maybe even a lot of money. But if you take records away from a hospital, the staff might end up hurting the patients it works so hard to protect. This isn't just a question of money anymore. We have human lives at stake."

"My people are fighting this with everything we've got," Jacob responded defensively. "Given enough time, we can regain control of the system. Then we'll upgrade security to make sure nothing like this ever happens again. We'll install a network-based infection detection system. From now on, just warding off intruders isn't enough."

"The question is, *When* can we win?" Paul said quietly, holding down his frustration. "We can't go without records much longer."

"This is the digital equivalent of hand-to-hand combat," Jacob replied. "We know the system better than these people do, but they have the advantage of

surprise. I just can't tell you when we're going to win. There isn't a quick fix for a problem like this."

Paul nodded toward the screen. "They've offered us a quick fix," he said.

"You're not seriously considering paying these guys, are you?" Jacob asked incredulously. "If we pay once, we'll be a target forever. Don't do it. It's not right. We can beat these guys, Paul. Just give me some more time."

A Ticking Bomb

"Paul, we need to make this go away," said Lisa Mankins, Sunnylake's head legal counsel. Her hair was pulled back smoothly, and she was dressed as usual in an austere pantsuit, but Lisa looked as if she'd just undergone hours of torture.

After the hackers' latest e-mail, IT had managed to restore the system twice, only to have it crash minutes later. Despite the department's best efforts, Jacob explained, the hackers kept regaining access. Most of the staff was beginning to look emotionally drained. The hospital had ordered all doctors to write paper nursing orders and prescriptions for the time being. The younger doctors, who'd always relied on EMRs, were baffled by the concept. Even some of the older ones had forgotten how to scratch out "500 mg Amoxicillin" legibly.

Paul had called Lisa into his office to talk about damage control.

"Our legal exposure in this kind of situation is mind-boggling," she said. "The longer this goes on, the bigger the risk. Literally every second is a liability. Doctors are resorting to old paper records for the most urgent cases, but those records are way out of date. Earlier this afternoon we treated a patient with medicine he was allergic to. Luckily, his reaction was mild – but we may not be so lucky next time."

Lisa paced back and forth in front of Paul's desk. "We have to assess our options. It doesn't look to me like IT can fix this problem fast enough – if at all."

> "Our legal exposure in this kind of situation is mind-boggling," she said. "Literally every second is a liability."

"The way Jacob explained it to me, IT needs a certain amount of time to regain control," Paul said. He had tried all morning to preserve his confidence in Jacob's ability, but it was beginning to fade. Each time the system was restored, hope had soared in Paul's chest, only to crash again when *Access denied* reappeared on every screen.

"We don't have that time," Lisa insisted. "You know that." After a moment of silence she spoke again, her face tight. "We have a budget for this kind of thing, you know. An acceptable-loss budget. We have insurance that covers IT risk and the money to pay these guys. Malpractice suits could cost this hospital hundreds of thousands of dollars in legal fees alone – and possibly millions in damages. A hundred thousand bucks pales alongside the losses we might face if we wait this out. I think it's practical – even moral – to pay the ransom. The longer we wait, the more we risk seriously hurting our patients and ourselves."

"I don't like the idea," Paul said. "Not at all. It's unprincipled to reward extortion. It would just encourage these people, and maybe lead to other attacks on other hospitals." He paused. "But it might be all we've got."

Lisa had barely left his office before George Knudsen, the chief of staff, stormed in.

"When are you going to fix this?" he demanded. "Do you have any idea what this will do to our reputation if some newshound gets wind of it?" George was a grizzled and intimidating fixture at Sunnylake. He'd been there for years when Paul arrived, and might well outlast him. The two had butted heads over the introduction of EMRs, but had been cordial since the initiative's success. George looked anything but cordial now.

"Everyone is working as hard as possible," Paul replied. "It's been tough for all of us."

"I don't think you know how difficult it's been," George said angrily. "You wouldn't know that unless you had to treat patients while wondering whether you were actually doing them harm. You wouldn't know that unless you were afraid of breaking your oath just because some young computer geek thought his system was a whole lot stronger than it actually is."

"George, you know how good the electronic system has been for this hospital," Paul retorted, alarmed by the older man's fury. "You admitted it yourself."

"I didn't know what kind of cost we were going to pay!" George roared. "You're making your entire staff look incompetent – or worse! Paper might have been slow, but it was reliable. If you don't fix this soon, Paul, I'm never touching one of those damn devices again. And I know plenty of others here who will feel the same way." He stalked out.

• • •

Paul lay on his back on the sofa in the staff lounge, staring up at the half-lit ceiling. It was 1:00 AM. The IT team was still in the hospital, waging cyberwar with the unseen adversary. The pattern of brief victory followed by defeat had continued into the night. Jacob had tried every online decrypter he could find; his team was fanned out across the hospital, scanning computers for leads.

Paul clenched his eyes shut. He kept seeing cinematic images of Allied code breakers battling the Germans' Enigma machine. Sunnylake's situation felt every bit as urgent. Try as he might, he couldn't clear his mind and let himself fall asleep. Crushing guilt, a sense of responsibility for all that had passed that day, pressed down on his chest.

Even after three years of success, during which the staff had almost without exception come to appreciate the efficiency of EMRs, Paul could clearly remember how hard he'd had to fight to get the system installed and accepted. Unless he could resolve this crisis quickly, he would lose all the ground he had won. The doctors at the hospital had been a stubborn, resistant lot at the outset, and George Knudsen wasn't the only one who would snap into I-told-you-so mode. It might be nearly impossible to get them to trust the system – or him – again.

If he paid the hackers – just this once – Sunnylake could make security the number one priority and ensure that nothing like this ever happened again. Paul rolled over, sighing. Was he actually considering paying extortion money to these criminals?

How should Sunnylake deal with the attack? Three commentators offer expert advice.

Caroline Eisenmann *is a former intern at HBR.*

> The first step should be to hire an emotionally neutral negotiator who can open a dialogue with the hackers.

DISTASTEFUL AS it may sound, I would suggest that Sunnylake Hospital go ahead and pay the ransom demanded by the extortionists. (This assumes, of course, that the threat is real and that there is a verifiable risk to patient health.) That may well be the only way that Paul Layman can keep Sunnylake's patients from harm and avoid the massive liability risk that Lisa Mankins, the head counsel, so fears.

Why would I recommend this? As a CEO, I had to deal with an analogous situation in November 2008, when Somali pirates in the Gulf of Aden attacked a $15 million ship belonging to the Clipper Group. The pirates held its 13 crew members hostage for 71 days. I led the emergency response team that was charged with ensuring the safety of the ship and crew.

Dealing with extortion is not part of a CEO's job description. In our case, the criminals held all the cards. During the showdown I learned that Somali piracy is a well-run business that includes a number of actors and investors. Though the pirates can make life unpleasant for the hostages, harming them is out of the question – that would be death to the pirates' business model.

The pirates knew that time was on their side. If we chose not to pay, they would simply hang on to the ship and crew; their well-honed system makes it easy to continually resupply the ship. (Although Danish law prohibits paying ransom to terrorists, there is nothing to prevent a shipowner from paying pirates.)

No CEO can hold out indefinitely against constant hammering by desperate relatives, an anxious press, and demanding politicians – it's simply not sustainable. In the end, we had no choice but to pay the millions of dollars the pirates demanded. (Insurance covered the cost.)

In Paul's case, the first and most important step should be to hire a good, emotionally neutral negotiator who can open a dialogue with the hackers and keep them involved in conversation, so that they will be unlikely to do even more mischief.

As the process moves forward, the negotiator can pass information between the two sides, while Jacob Dale's IT team works on getting the system running and then beefs up the security and emergency plans it should have had in the first place. Meanwhile, the police and forensic specialists can try to track down the criminals and put a stop to their enterprise.

Once negotiations are in play, everything turns into a chess game. The negotiator and the emergency team can work out terms and logistics. When an agreement has been reached, the money is dropped and the whole episode is over.

Another question is, What about the media? Chances are good that reporters will somehow find out about what has happened at Sunnylake. In our case, we decided to deal with the media very directly in order to help raise awareness of the threat that Somali pirates pose.

If shipowners come to understand the pirates' business proposition and are ready to do the hard negotiation necessary, they will be much better equipped to deal with the threat. During the negotiation process, we learned a great deal about where the ransom money goes and how it is used – and the authorities are now putting that information to good use.

Per Gullestrup *(pgu@clipper-group.com) is the president and CEO of Clipper Projects in Copenhagen.*

Wendy Wray

Richard L. Nolan *(rnolan2@u.washington.edu) holds the Philip M. Condit Chair at the University of Washington's Foster School of Business. He is a coauthor, with Robert D. Austin and Shannon O'Donnell, of* Adventures of an IT Leader *(Harvard Business Press, 2009).*

THIS CASE is an example of the kind of attack to which every organization, small or large, is now vulnerable. All organizations depend on technology; none are immune to the hordes of people around the world who seek to disrupt their operations – sometimes just for the fun of it and frequently for malicious reasons or personal gain.

This means that the CEO and the board are responsible for "good business judgment" in guarding against the threat. Paul's first mistake was to dismiss the original e-mail message. All IT threats should be taken seriously; had he had his wits about him, he would have let Jacob Dale know about it immediately. No IT system is "bulletproof."

Moreover, organizations need a plan for when they are unsure of the extent to which their systems have been compromised. Sunnylake should have had a workable, fully tested backup system to ensure uninterrupted patient service and protect everyone affected. Doctors and nurses are trained to diagnose, problem solve, and dynamically treat their patients. IT systems facilitate, but are not substitutes for, patient treatment. The fact that the hospital did not have up-to-date security software installed, or a reliable security outsourcer and an emergency plan in place, is inexcusable.

As bad as it seems, this crisis is easier to deal with than other, vaguer threats (such as robotlike software programs that randomly alternate between dormancy and sabotage or stealing customer data), because Sunnylake knows there has been an intrusion: Someone seems to have changed the access security.

So what should Paul, the CEO, do? First, he had better get off that sofa and give up the vain hope that IT can restore the system and get the hospital running again. When hospitals in CareGroup, a team of health-care professionals in eastern Massachusetts, experienced a similar situation in 2002, the CEO, the CIO, doctors, nurses, and the support staff began operating just as they had in the 1970s, before their integrated EMR system was installed. The professionals who remembered what that was like coached those who had always depended on computers. As John Halamka, the CIO, told his board, "The good news is that health care did not suffer."

Paul should also be in high communication mode with all of his constituents. He should understand that in today's networked environment there are absolutely no secrets. Any IT breach forces an organization to ask, How much should we disclose about this threat? In this situation Paul needs to provide full disclosure to his various constituents: employees, board, patients, and the public.

In no way should he acquiesce to the demands of the extortionists. There is no guarantee that they haven't embedded further corruption in the system. The code needs to be examined line by line and thoroughly cleansed. The hospital's network infrastructure and other IT systems must be analyzed for possible corruption and protected with updated security software.

Finally, Paul needs to face up to the fact that he may lose his job. After all, he is responsible for all the strategic resources of the hospital, including IT. The board should also be held accountable for the lack of strategic oversight.

Sunnylake Hospital's case offers an advance warning about a very serious emerging problem for all chief executives and their boards.

> Paul needs to provide full disclosure to his various constituents: employees, board, patients, and the public.

Peter R. Stephenson *is the chairman of the department of computing and the chief information security officer at Norwich University in Northfield, Vermont.*

IF YOU'VE festooned the windows and doors of your network with garlic, hung up mirrors and crucifixes, and splashed everything with holy water in the form of firewalls, antivirus software, and so on, you'll probably be safe from vampires – hackers or malware. But in this case, preparations for a security breach were lacking, and some gumball – possibly someone shopping online from a computer connected to the network – may have let the vampire in.

Unfortunately, data security is an afterthought in many hospitals. Recently I walked past a hospital's information kiosk, which was supposed to be staffed by a volunteer. The computer was on, the screen was lit up, but nobody was around – a gross violation of U.S. law protecting patient privacy.

At Sunnylake the system keeps crashing because the attackers find a new way in every time a fix happens. This may be because the malware – the evil program that facilitated the breach in the first place – has relayed a message back to the hackers, letting them know what Jacob and his team are doing.

If Paul had let the IT people know the moment the first nasty message arrived, they could have taken the system off the internet immediately, ensuring that a rogue program related to the attack couldn't get in from outside. This would also have blocked any back doors the hackers had created.

Next, they should have verified that the bad guys had actually gained access to the network. It's not unusual for an extortionist to send a threatening message in hopes of scaring the recipient into a payoff. Jacob and his team should have checked the system logs to see if changes had occurred. If they had reacted immediately, they could have forestalled the second e-mail or additional penetrations.

How can IT fix the network? First, the system administrators need to regain their passwords and recover control. At the risk of getting technical, this means shutting down servers, performing a secure delete on all the server disks by deleting and overwriting with random data, restoring the servers and the data, and making sure the security programs are fully updated and operational. IT needs to run a malware scan on every workstation in the hospital, in case the attack came via an employee computer. Though labor-intensive, this scan is critically important.

What about the extortionists? The e-mail messages offer some tantalizing hints as to their identity. The use of the abbreviation "u" for "you" suggests a young person or a foreign national with poor English skills or an amateur who downloaded the attack program from the internet. It's also possible that the bad guys are quite intelligent – and it's always safer to overestimate hackers' skills. They may not even be "outsiders." A vengeful employee or patient who happens to pass by an unattended workstation can do plenty of damage. Before reconnecting to the internet, Sunnylake should watch what happens for 24 hours. If the attackers are insiders who retained access to the system, they may try to get in again.

Even if Paul hires a security consultant, which is a step I would recommend, it's unlikely that the hospital will find the attackers. Still, the consultant can help build a profile of the attackers, improve security, and train key personnel, so that Sunnylake can protect itself in the future.

IT needs to run a malware scan on every workstation in the hospital.

Reprint R0910B
Reprint Case only R0910X
Reprint Commentary only R0910Z
To order, see page 143.