

Bluestein wondered what he should tell the people at Commerce. Should he be candid about the company's untimely security lapse? Commerce was one of TTI's most security-conscious customers, and hence this revelation might jeopardize lucrative future contracts. However, Commerce was told last week that the project was done and that they would receive it right on time. How, then, could he explain what could have gone wrong to delay delivery by several weeks and maybe longer? Also, Bluestein wondered about the corporation's legal and moral responsibility for what happened. Chase was clearly the main culprit here but to what extent was the corporation also liable for his transgression? And if the company is liable, should it make some restitution to its customer whose business is adversely affected because of this mishap? Bluestein began sorting through all of these questions as he stared at the pink phone messages in front of him.

Case 7.2 Internet Abstinence (A)

Jonathan Fuller, Director of Operations at Higgins Psychiatric Hospital, was handed a copy of the *New York Times* by his assistant as he entered his spacious office. She called his attention to several relevant stories including one on the business page. As Fuller settled into his chair, he perused the lead story in the business section with the headline, "Experts See Hackers Gaining an Upper Hand in Fight over Security." The article described in some detail why computer security experts were convinced that corporations were losing ground to the electronic thieves who were breaking into public and private computer systems. Every time one hole was plugged up new ones seemed to emerge.

This was the latest in a long series of articles in the press that articulated the same concern. There seemed to be a growing consensus that security on the Internet was a fleeting illusion. Dr. Fuller put the article aside and wondered how any organization could insulate itself from the dangers of electronic intrusion in this age of openness and connectivity.

The Higgins Psychiatric Hospital was located in a beautiful, but small and obscure town in western Vermont. Among the rolling hills and verdant pastures one could find a discrete edifice which housed some of the finest medical professionals in the entire world. One could also find numerous wealthy and famous individuals among the many patients in this august hospital. Higgins was a haven for celebrities, and, as a result, it had developed over the years a security consciousness that permeated the hospital's decision and policy-making processes.

Like other administrators at Higgins, Fuller was a medical doctor by training. After working for several years as a specialist in the medical profession he decided to become a hospital administrator. He took a job as an associate director at a large teaching hospital in Boston. During his stay at this hospital he also earned an MBA degree at one of the local universities. When the job at Higgins opened several years ago, he saw an opportunity for advancement and sent his resume to the search committee. They were impressed with Fuller's background and experience and offered him the position. What especially impressed members of the committee was Fuller's background in technology and his vision of how technology could make the hospital's operations more efficient. Consequently, when he took the job he was charged with bringing Higgins's antiquated computer technology "into the twentieth century."

Fuller was convinced that he had made great strides toward achieving this challenging goal. He had carefully developed the hospital's information technology architecture and established guidelines and policies for the use of IT resources. He threw out the hospital's outdated computer system and replaced it with a more contemporary and versatile infrastructure: client/server technology using an IBM mini-computer as the host linked together with IBM PCs and other compatible machines.

Once this new system was installed, Fuller began working with the hospital's small MIS staff to work out plans for the development and enhancement of some critical applications. These included a patient tracking and billing system and also a scheduling system for the physicians who dealt with outpatients. At the heart of this system was the patient data base, including personal data and medical histories.

Most of the physicians at Higgins had never laid hands on a computer before Fuller's arrival. However, in an effort to make computing technologies pervade the hospital environment, Fuller required every physician to schedule his or her appointments using the automated scheduling system. As more and more doctors became comfortable with using their IBM personal computers they began using the e-mail facility, wordprocessing programs, and other packages that were available on the host system.

Overall Fuller and the hospital administration were quite pleased and even astonished at the progress that had been made in this critical area. But progress has a price and Fuller now faced a thorny decision about the future direction of the IT system at Higgins. During several recent meetings of the hospital's operations committee, which was chaired by Fuller, some of the more technically sophisticated doctors

voiced their opinion that it was time that Higgins took the next step and connected to the Internet. One or two doctors admitted that they were using modems to connect to the Internet in order to communicate with colleagues in other hospitals. They felt that the time had come for Higgins to provide for greater Internet access. As one of the staff physicians put it, "As I see it, connecting to the Internet is inevitable. There are just too many benefits that we are foregoing by not being on the network. For one thing it's becoming increasingly difficult to stay in touch with our counterparts in other hospitals, since this is the way they communicate and share valuable information." The head of the research division echoed this sentiment: "The Internet is vital for sharing our research with other institutions all over the world. There's no doubt in my mind that this connectivity will greatly increase our productivity." Other physicians on the committee, though still novice computer users, agreed with this assessment and encouraged the hospital administration to expand its vision and connect to the Internet.

Fuller was certainly sympathetic with these persuasive arguments. There were many advantages to the worldwide access that the Internet provided so easily and inexpensively. However, this was not a simple decision. He was deeply worried that making this connection would just be too risky. His biggest concern, reflected in the news articles he had been reading recently, was that hackers could penetrate the hospital's private network to steal or tamper with confidential patient data. Or they could possibly eavesdrop on information being exchanged with those outside the hospital. What if a Higgins physician was communicating with another physician about a particular patient's problems and the communication was intercepted by an unscrupulous hacker?

Thus, his major concern was the extraordinarily sensitive nature of the information stored on the host system: private medical records. Also, since Higgins continually had many celebrities in its midst, it was imperative not to put their privacy in jeopardy in any way. What if an intrusive hacker were able to penetrate one of the hospital's patient data bases and tap into individual medical records? The potential ramifications were chilling.

Fuller and several others voiced these concerns at the committee meeting but for the most part they fell on deaf ears. Many were skeptical about his arguments that the system could not be made secure. They also felt that to a great extent the tremendous benefits of greater connectivity far outweighed the small risks of intrusion. They seemed to believe that the administration was just being overly cautious and conservative. In their view, this was the way of the future—a simple and

convenient method of communicating with colleagues and fellow researchers all over the world.

After several other meetings and extended debate on this proposal, Fuller realized that he faced a difficult decision. Sometimes the debate became heated and at one meeting Fuller was called a “paranoid alarmist.” He had been considering the alternatives for several weeks but was no closer to a resolution of the conflicting issues. He was still worried that the hospital might be liable for a security breach. Also, would others look upon this decision as irresponsible and short-sighted if hackers were able to intrude the hospital’s network and retrieve sensitive information about one or more of its patients?

As he reflected once again on this difficult problem, he recalled the advice from one of his counterparts at a nearby medical hospital: “The Internet is wonderful, but let’s face it, it provides no security and no measures to protect privacy or data integrity.” There were certain security measures that could be taken such as the construction of a “fire-wall” but even this was not foolproof and it was also fairly expensive.⁵ Given the hospital’s budgetary constraints, there might not be adequate funding at the present time to provide this level of security.

Fuller wondered whether he *was* being too conservative and apprehensive; perhaps he should be a bit more permissive and recommend the connection. Or should he continue with the strategy many in the hospital had now dubbed as “Internet abstinence?”

Internet Abstinence (B)

Fuller concluded that he needed more information in order to make a more informed decision. He arranged to hire a security consultant to review the hospital’s present security and offer some advice on the feasibility of connecting to the Internet. After studying the hospital’s situation for several days the consultant submitted a detailed review to Fuller. The following are the main points of his extensive report:

- Present security is quite adequate but connecting to the Internet brings a whole new level of risk to the organization for which it may not be fully prepared, technically or culturally.
- The Computer Emergency Response Team (CERT), a federally funded organization that keeps watch over the Internet, has recently issued an advisory describing a rash of recent break-ins at several major hospitals; these have allegedly been orchestrated by a group of hackers who want to demonstrate the poor security systems of the medical establishment.

- If the hospital decides to connect to the Internet it must implement state of the art security such as a well-configured application-level firewall, which will create a subnet or separate zone between the internal network and the Internet. It includes a router (or gateway) between the internal network and this zone and between the zone and the Internet. These routers, configured according to internal security policy, are designed to filter out unauthorized entry into the network. Estimated cost (including installation and configuration): \$60,000.
- This firewall will harden the system against potential damage from an intruder but it is not foolproof. No system can be made absolutely secure, but with a robust, high-level security system the risk of intrusion can be minimized.

Fuller pondered this report during his brief lunchbreak. It was Friday afternoon and he was determined to bring this matter to closure sometime next week. It had already consumed too much of his energy and attention and he was anxious to move on. The consultant's analysis and security review were certainly helpful but he still had many substantive questions.

He was also deeply concerned about the *process* of making this decision. He knew where many of the hospital staff stood on this matter but what about the patients whose personal data was at stake and who were most at risk from security breaches? Should they play some role in this decision and, for that matter, in other security decisions? Should he consult the hospital's advisory board which included several patient representatives, or would the discussion of this matter cause unnecessary anxiety and alarm?

Fuller began to reread the consultant's report as he thought about how to respond to these questions.