REAL WORLD CASE 2

Geisinger Health Systems and Du Pont: Security Management

Whether balancing the needs of security with the push for greater access to data, coping with government mandates, or planning for possible budget cuts, IT security managers have their hands full. Frank M. Richards has been scrambling to deal with those challenges. As CIO at Geisinger Health Systems (www.geisinger.org), a health care network in Danville, Pennsylvania, that serves more than 2 million people, he faced an April 2003 deadline for compliance with the U.S. Health Insurance Portability and Accountability Act (HIPAA). The law required health care organizations to safeguard patient data from unauthorized access and disclosure. But HIPAA set goals without giving specifics on how to get there, so Richards had to balance the legal requirements with a demand from health professionals for ease of access—a daunting challenge.

"This can be particularly problematic in the medical field, where care providers are under tremendous time pressures," he says. Understanding workflow, assessing risk, and educating users are all key components of a security system that achieves the correct balance between access and control, he says. Geisinger's Electronic Medical Record (EMR) program focuses on easing access to data. It lets physicians at 50 clinics use mobile devices to order medications, receive alerts, enter patient progress notes, and communicate with patients. Another program, MyChart, lets patients access their medical information via the Internet.

Both programs raised security issues. For example, security needs dictated that the database that powers MyChart be installed on hardware separate from the EMK system. Richards's staff is also evaluating biometric and proximity devices as ways to streamline secure network access. And caregivers accessing patient information via the Internet will be required to use electronic token identification in addition to a virtual private network or other encryption method, he says.

Richards expects security technologies such as intrusion detection systems to finally begin delivering on their promises. "Inadequate analysis tools, incompatibility with existing network management software, and inability to handle large volumes of data have combined to keep us from deploying these security tools until very recently," he says.

Du Pont Co. Process control networks are one of the essential applications of IT in manufacturing environments. For example, more than 2,400 oil, natural gas, and chemical companies in the United States employ process-control networks in their manufacturing systems. Other heavy users of process networks include the power, water, food, drug, automobile, metal, mining, and manufacturing industries. For example, process networks in the chemical industry control chemical-making equipment and monitor sensors. If anything goes wrong, such networks react by adjusting the environment in predefined ways, such as shutting off gas flow to prevent leaks or explosions.

One company that's taking process network security seriously and involving IT is Du Pont Co. (www.dupont.com) in Wilmington, Delaware. Tom Good, a project engineer at the chemical manufacturer, has been leading its 20-month-old effort to categorize and reduce its process-control system vulnerabilities. Du Pont's philosophy for dealing with this problem, he says, is that "On all of our critical manufacturing processes, we are either going to totally isolate our process systems from our business systems by not connecting our networks, or we're going to put in firewalls to control access."

To tackle process-control network security, Good says Du Pont formed a team made up of IT staffers, who understand networks and cybersecurity; process-control engineers, who understand the process-control equipment; and manufacturing employees, who understand manufacturing risks and vulnerabilities. To give the three groups visibility, each reports to a separate member of a committee that's leading the effort. The team first discerned which control devices are critical to manufacturing, safety and continuity of production. Next the team identified the assets of each—hardware, data, and software applications—then researched relevant vulnerabilities. Only then did it begin the arduous task of testing fixes and workarounds to see which ones might work for which machines.

Even in a manufacturing environment that uses similar process-control hardware and software, precise vulnerabilities differ by environment. "Dealing with a water treatment process on effluents out of a plant is considerably different than dealing with a production operation, where you might be dealing with vessels under high-temperature and high-pressure conditions," says Good. On the basis of its research, the team is also deciding how to separate networks and where process-control firewall appliances should go. "The greater cost is in the network equipment and reengineering activities to separate networks and place critical process-control devices together on the clean side of the firewall," says Good. "The challenge for us is to accomplish these tasks while keeping the processes running."

Case Study Questions

1. What is Geisinger Health Systems doing to protect the security of their data resources? Are these measures adequate? Explain your evaluation.
2. What security measures is Du Pont taking to protect their process-control networks? Are these measures adequate? Explain your evaluation.
3. What are several other steps Geisinger and Du Pont could take to increase the security of their data and network resources? Explain the value of your proposals.

Sources: Adapted from Dan Verton, "How Will You Secure Your Company Data?" *Computerworld*, January 6, 2003, p. 24; and Mathew Schwartz, "Wanted: Security Tag Team," *Computerworld*, June 30, 2003, pp. 38–40.