My old friend Stacy and I were chatting last week about the parlous state of her company's business continuity planning. Stacy works in a sizable manufacturing plant where they make left-handed gizmoplazes for the export trade. She's one of the sales managers there and supervises 50 sales staff, of whom about 15 are usually in the office at any one time (the rest are on the road visiting customers except on meeting days).

It seems that a couple of weeks ago, electricity failed at around nine o'clock on Monday morning. All of the company servers are safely connected to uninterruptible power supplies (UPSs), so there was no damage to the equipment or to the data. The UPSs allowed a graceful shutdown, but there was insufficient power for continued operation.

The mains power came back at about 11 o'clock that morning. The servers stayed down until 1 pm that afternoon.

Stacy called the help desk to find out what happened: why weren't the servers coming back up now that the power was restored?

The answer shocked Stacy even though she is not by any means a technically sophisticated person; she is, however, smart. Here is what she learned.

The servers were not allowed to come back online because the batteries on the UPSs were drained. It took another two hours to recharge them; therefore, the servers were down until 1 pm.

And why were there no secondary UPSs? Nobody knew.

What about an emergency generator? That would support continuous operation. Well, it seems that the IT managers had asked many years before for an emergency generator that could kick in quickly when power failures lasted more than a few minutes, thus allowing servers to stay online. Since all of the sales staff are equipped with laptop computers, they have at least a few hours of self-contained power that would allow them to work even without mains power in the office as long as they had access to the databases and Microsoft Exchange e-mail server. The off-site sales employees could also continue working as long as the network servers were accessible.

So it seemed clear to the IT staff using elementary risk analysis that maintaining the continuity of service of their servers ought to be a high priority for the factory. They wrote up their proposal for an emergency generator and the appropriate isolation switches and waited for approval of the relatively moderate outlay (around $50,000 capital cost).

Unfortunately, their analysis was initially rejected by the factory directors. The factory was still largely under the control of old-time entrepreneurs who had founded and grown the business as a family enterprise a generation before. They were used to taking risks and they didn't like the size of the proposed expenditure, especially for what they perceived as secondary issues such as office work. How could access to computers possibly be mission-critical?
The IT department persevered, however, and after a couple of years they finally got upper management approval for purchase of an emergency generator. Unfortunately, Stacy also learned through the grapevine that the founder's son-in-law had a fit about installing the generator on the roof, which had been identified as the best location for the generator. The scuttlebutt was that he thought it was so hideous that it would make the factory building looked too ugly. He therefore prevailed on the board of directors to maintain the generator as a portable device on a trailer and drag it next to the IT department only when required. This process usually took a couple of hours and was dependent on a single employee who knew how to hook up the generator -- and he wasn't always around. As a result, the generator they bought was almost never used.

In addition to the sales staff who were inconvenienced by the server downtime, several hundred other employees dependent on their tower computers were completely down during the four hours of system unavailability. There was absolutely no provision for providing emergency power to those employees. The factory doesn’t even have contingency plan to allow them to respond to customer phone calls; in fact, their digital public branch exchange (PBX) is on the same UPSs as their servers, so they lost outgoing phone service, inbound phone service and voicemail all at the same time -- not exactly great for the company’s public image.

Stacy said that the worst part of the whole situation is that nobody in the upper management gave the slightest indication that they were even aware of the problem.

The remainder of the analysis is left to the readers.

[All details changed to protect the guilty.]

* * *


M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance <http://www.msia.norwich.edu> at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mekabay@gmail.com>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2006 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.