


Debate: Was IT too controlling or was this employee out of line?

by Ray Geroski | Feb 05, 2003 8:00:00 AM

TAGS: Linux, Strategy, NETWORKING, SECURITY, Ray Geroski, IT Department, information technology

87 comment(s)

- Email
- Save
- Print
- Digg This
-

 **Takeaway:** Did IT act appropriately in locking down the equipment of an employee who refused to play by the rules? Many readers of a recent article said that the IT department was being too stringent. Find out how others reacted.

A recent NetAdmin Republic article examined the case of an employee who repeatedly circumvented IT policy to work independently on a Linux project designed to save the company some money. The IT department responded to the employee's infractions by locking down his machine and network connection to prevent him from violating the rules he'd agreed to follow. Members responding to the story were, for the most part, divided into two camps: One saw the IT department as too controlling; the other viewed the employee as a security threat who should have been fired for repeatedly disregarding policy.

However, some members said that all parties involved, including the IT department, the employee himself, and company's management team, shared the true blame for the debacle and the employee's failed project. They contended that the incident could have been avoided altogether had those three groups worked more closely and communicated more clearly at the outset.

IT zealots

Many members were highly critical of the actions the IT department took in response to the employee's transgressions. They felt that the IT department was simply being too controlling and not allowing the associate the freedom he needed to work on his project.

Greg Searle, for example, wrote, "I would not want to work with a company with such a restrictive policy. I know that IT needs to keep things secure and working, but at what point do you give up innovation and creativity in the name of security?"

Searle, like many others, thought that the IT department went too far in controlling what the employee was able to do. Member **Radiolandog** said, “The IT department depicted seems intent on stifling creativity.”

Some also felt that the IT department’s actions were actually detrimental to the company.

“I kept waiting for the part where the new employee stole data, planted a virus, or some other nefarious scheme,” **Fingerpicker** said. “Instead, all I found were minor policy violations that frustrated the efforts of a creative individual and killed a project that could have provided a cost savings to the company.”

Since the employee did nothing deliberate or overt to sabotage or compromise the network, many felt that he was being unfairly targeted as if he were a hacker. Member **Perseus**, a network admin, said, “I am totally and completely against the kind of treatment meted out to the newbie. This is a totalitarian policy. As stated by other members, this resulted in only one thing, that is, it killed the Linux project.”

A number of readers pointed out that the IT department is a service organization whose purpose is to support the user. As such, the department failed to do its job in providing the new associate with the tools necessary to complete the special project. Perseus said, “If I were the administrator in this company and something like this happened, I’d consider it as my own personal failure to support the newbie.”

Security policy

Not everyone was so quick to come to the employee’s defense. Many said that he should’ve been fired immediately for skirting policy and repeatedly failing to abide by the rules that had been laid out for his work on the Linux project.

Member **Mogliak** asked, “What type of company is this?” and argued that “[At] most places, this guy would have been fired or been taken off the project right away.”

Several members agreed with this stance, among them **Anthea**. “I work for a police force, and there is no way this employee would have kept their job for so long—we have let IT staff go for less infringements than that. We work with highly sensitive information and cannot take any chances.”

Others defended the IT department’s response to the associate’s actions, noting that it was IT’s responsibility to manage any hardware and software installed on the network.

Adam Aube said that because IT is responsible for all network hardware and software, it must also have the authority to control any changes to software and workstations that might affect the network. In this case, the IT department was exercising its authority to halt the use of network resources in a manner that violated company policy.

Others saw the employee's actions as more than just possible security breaches. They were highly suspicious of the associate's motives as well as his repeated excuses for his actions.

For example, **One Pro** pointed out that the biggest security threats often come from within and that this employee represented an internal threat. "He was obviously and deliberately not following the rules, and you must not trust that kind of worker." One Pro added that the employee's excuses were just like the ones supplied by malicious employees who get caught.

Several members agreed that the associate's repeated infractions and quick excuses were indeed suspicious. Some suggested that the employee's efforts to circumvent security measures smacked of corporate espionage.

Management and planning

Between the two extremes of condemning the IT department for exerting too much control and praising it for reacting appropriately to a security threat were the voices of those who looked at the story from a broader perspective. They argued that the incident represented a failure on the part of all involved to document a plan, communicate effectively, and cooperate on the project. Many pointed to the management of the company, which failed to take the steps necessary to see that the project was properly carried out.

Member **Ddamon**, for example, felt that neither the associate nor the IT department handled the situation correctly. Ddamon said, "[IT] should have put the server on an isolated network in a test environment. Then the associate would have to work on the project in the IT department and not behind closed doors." This step, Ddamon argued, could have saved both parties a lot of trouble.

Member **builder77777** said that poor planning also doomed the project. "Hasn't anybody heard of the process of developing a system? Putting a bunch of stuff on a whiteboard isn't even close to proper software engineering techniques."

Iaind also felt that the big failure in the incident was a lack of project management and agreed that it should have been handled in a test or development environment to prevent it from becoming such an issue.

Many readers saw past the controlling-IT vs. innovative-employee issue to identify mismanagement as the real problem in the case. Had the whole project been managed more effectively from the start, they argued, none of the conflict would have occurred in the first place. The failures they pointed out highlighted how critical it is for management and IT to collaborate to ensure that employees can work effectively while abiding by company policy.