Yes, if proper permissions are not set up for users and files on the network, malicious users could use a variety of methods to crash a company’s network. Starting with disk, if given unrestricted access, users could delete key files that are required for the operating system (or key underlying applications) to keep functioning properly, or at all. This is assuming direct access, but the age old “delete system32” would basically accomplish this.

When it comes to memory, there are many instances of attackers either overloading systems due to a memory leak or grabbing data from memory that has not been properly secured. Heartbleed is an example of the latter where, due to an exploit found in a software library, attackers were able to grab unsecured memory and decrypt private information with it (<https://heartbleed.com>).

For the dangers of having unrestricted access to CPU I did not find as much. It seems to be much less common to use the CPU to exploit the system. That being said, I found this fairly recent article talking about how hackers abused a specific bit in an intel CPU called the trap flag so that they could evade detection(<https://www.itpro.com/security/malware/360299/hackers-use-single-bit-change-in-intel-cpu-register-to-evade-detection>).