When the pressure's on, it's tempting to cut corners. That's why we've rounded up the five most common ways IT Admins cut corners under stress, so you don't make these same mistakes.

Until the day comes that our systems achieve actual sentience, the possibility for human error will continue to pose the single greatest threat to any technology driven organization. The responsibilities of network and system administrators demand unlimited access to your most sensitive processes, and finding the balance between proper security protocols and system accessibility is an issue that every successful organization faces. Restrict access too heavily, and your team won't be able to do their jobs, but throwing open the proverbial doors will invite more than its fair share of trouble.

It is for this very reason that experienced admins who know how to navigate their systems while maintaining the best possible levels of security are worth their weight in gold, but even the best admins are capable of making mistakes when the pressure's on. Time constraints, exhaustion, and unforeseen but inevitable crises are facts of life in the modern workplace, and all of these factor into the occasional mishap. We've rounded up five of the most common mistakes that almost any admin might be embarrassed to admit they've made.

With all the measures we take to ensure our systems' security, it's easy to take the lowly password for granted. But there isn't an easier (or more embarrassing) way to forfeit the keys to your infrastructure than typing "password123" during your initial configuration. Because the security of even the most vital systems might be thwarted by a weak password, many organizations implement password best practices and policies, which should include two-factor authentication where possible.

Unfortunately, while two-factor authentication is becoming increasingly popular with end-user applications, it's not entirely ubiquitous at the admin level. Follow proper password practices for any system you configure, even if that system's just a quick test account on your public cloud infrastructure. Sure, someone might not be able to access your hypervisor through the virtual machine, but what's to stop them from initiating a DOS attack from within your network? Weak passwords in one part of your network, even on a virtual machine, can give attackers a foothold.

It's equally important that you not use repeat passwords. Your critical systems should all be protected by unique passwords—store them in an encrypted file or application, offline if at all possible—to provide optimal protection against brute force intrusion. While these systems are likely set up to lock out repeat password attempts, lower-

At DigiCert, we understand the challenges that IT administrators face. Many people make compromises when they're under stress and when the pressure's high enough, even veteran administrators make mistakes they'd never want to admit to. Reducing unnecessary stress through proper planning and testing will help you to keep a cool head for those unavoidable emergencies that inevitably pop up.

Another challenge that admins are constantly dealing with is the relentless effort by hackers to devise new and ever more sophisticated exploits. It's hard enough to manage your network security without the ground always shifting under your feet, but unfortunately it's just not that easy.

That's why we've created an arsenal of powerful security tools that evolve just as fast as the everchanging security landscape. And, since SSL is often your f ŧ T p' t, ws $ ì