IS YOUR ENYIRONMENT SECURE? Do you Do you Do you use Do you use use physical administrative use technical operational controls? controls? controls? controls? Sure Nah; we relish Yes the danger of sitting on critical updates for a Do you maintain week or more Nah Do all your Do you install patches Do you just mean inventory of your machines start with and updates quickly? locks and alarms? hardware and software a secure baseline? Do you remove access No, we're quickly when an Not secure. Not secure. Not secure. I'm watching Yes better than Yeah Yup Try PDQ Deploy. Try PDQ Inventory. Try SmartDeploy. employee leaves the employees company? brawl in the breakroom as we speak Do you have Do you provide Nope Do you use Nah Do you have CCTV? documented a high-quality regular cybersecurity cybersecurity policies? training sessions? anitivirus software? Do you dispose of old Not secure. Not secure. Not secure. Not secure. Most breaches are hardware, software, Your environment is Antivirus software is Go check the server Nope Yup Yeah Love them a lawless land ripe caused by human error. and data securely crucial to detecting room to make sure no You're playing with fire. for cybercriminals. and promptly? and quarantining one lives there. malicious code. Acceptable use, Nope That's a thing? No way Is that because Do you maintain Do you use a incident response, most of your team backups of critical files? network firewall? remote access, network Not secure. works remotely? security, etc.? You're hoarding policy count? treasures like Gollum. Not secure. Not secure. Backups help you recover Just hope that threat You're basically putting Definitely The works from human error, natural actors don't catch wind out a welcome mat for disasters, hardware of your trove. intruders. failure, and cyberattacks. We leave Administratively, you're Hard pass Nah Do you review Do you encrypt no trace in a pretty good place. audit logs regularly? sensitive data? But don't rest on your laurels. Full security Not secure. Not too shabby! Make requires a well-rounded Not secure. You're making sure to stay on top of approach. Audit logs make it intercepted data easy 🌈 physical controls by Yes Yeah easier to spot intruders to read. At least give repairing and updating and internal misuse. cybercriminals more equipment regularly, and of a challenge. don't neglect other So many plans Do you have business security components. Do you use an IPS continuity and incident Not secure. or an IDS solution? What's that? response plans? Using public Wi-Fi without a VPN is the That's some impressive technological equivalent planning and Not secure. of licking a trash can. Yes Definitely preparation! Clear Your network Don't do it. deserves better. procedures help ensure not Pajama pants are your success, but don't part of our official let them distract you to company uniform When employees Nope other facets of security. Not secure. connect to public Balance is critical. If things go wrong, you networks, do they need to act quickly to use a VPN? prevent further damage and continue normal 100% of operations. Don't waste valuable time scrambling the time for solutions. Sounds like a hassle Of course Do you also actively manage Your technical security Follow each of the four central nodes. If you get to the mobile devices? is admirable, but if green bubble in each path, congratulations! But you're not using PDQ Layered authentication is my life's passion Deploy & Inventory, No remember that cybersecurity is not a one-time effort. Not secure. Do you use MFA? SmartDeploy, and Try SimpleMDM. Continuous improvement is critical for sustaining a SimpleMDM, you're probably putting in strong cybersecurity posture. more time and money Not secure. than necessary. Are intruders accessing your critical data? Who knows?