Edwin Chen, Marissa Ventresca, and Griffin Vella
Ethics Essay
NSSA.221.02/05/L1
11/25/2024

A system administrator is asked to deploy a new software package that has yet to be thoroughly tested and may pose a risk to the stability and security of the system.

The USENIX Code of Ethics (CoE) for System Administration is a framework for professionals in the field of system administration. It emphasizes the principles of integrity, respect, and responsibility. Users in the field must commit to fostering an environment that values ethical understanding, behavior, and technological advancements for the individuals who will utilize the work they create. The CoE promotes professional conduct while ensuring collaboration and innovation within the workspace. Our professor, who experienced this situation firsthand in his career as a system administrator, provided us with the prompt above. He asked if the following violated any of the CoE, and we concluded that it violates several of its principles. However, the following will focus on communication, Privacy, and system integrity violations - all of which are majorly impactful on any company or organization's success.

The scenario violates the communication ethic because it undermines the principle's definition of transparency and honest communication between the system administrator and the clients. The CoE defines *quality* as "Communicate clearly, respectfully, and honestly…Provide sufficient information to others to make informed decisions about technical or ethical issues". The system administrator is responsible for communicating the potential risks and limitations when deploying untested software. Since the prompt does not state that the system administrator addressed/voiced these concerns, the admin has failed to ensure informed decisions and client consent that the deployment will impact. When the system administrator withholds

communication, the potential risks impact client trust and collaboration. Following ethical communication demands openness and honesty throughout the development process to ensure decisions are in the best interest of the clients, users, and the organization. The lack of transparency between the client and system administrator not only jeopardizes the completion and success of the project but also compromises the integrity and ethical standards expected of professionals in tech-related fields. If a system administrator fails to unveil the risks to their clients and users, they will have disregarded their responsibility to uphold trust and potentially damage professional relationships. Communication is a necessary tool that all levels of internal affairs must practice, and the customer must be informed to illustrate intent and effect concisely.

Privacy is a sacrificed trait within this prompt as well, as an update that is compromised and, as stated above, "may pose a risk to the stability and security of the system" will be one that allows for the system to lack proper infrastructure designed to keep information safe. This quality of instability and risk exposes weak spots that malefactors could exploit for data, including company, executive, and individual information. All aspects mentioned before may contain highly susceptible content that will be detrimental to the organization if negatively utilized or leaked. In Chapter 12 of Limoncelli's book, he claims, "Procedures should be defined for what to do if privileged access gives someone information about something that would not have otherwise been made public." Privileged access is integral to the company and a critical point that System Administrators should take seriously, especially if undermined via potentially compromising visibility - therefore directly defying Limoncelli's warning of the proper procedure for sensitive information. Rather than risk publishing work that might be easily accessible and exploitable, If even the visual reception of some private information requires a procedure or policy, this would be reason enough for the system administrator to demand a halt

on implementing a software package that could cause this issue tenfold. The CoE also attests to this assessment, as the implementation of the software package violates its privacy clause: "access private information on computer systems only when it is necessary in the course of my technical duties. I will maintain and protect the confidentiality of any information to which I may have access, regardless of the method by which I came into knowledge of it ". The maintenance and protection aspects are forgone when installing an insecure and untested update. If the System Administrator chose to do so without further investigation, it could result in a significant privacy breach. *Privacy* is a vital quality that System Administrators cannot forfeit for speed.

System integrity is the final of the most concerning ethical issues that following through with the prompt would cause. In regards to the code of ethics, both clauses are violated by implementing an insecure software package, specifically, "to ensure the necessary integrity, reliability, and availability of the systems for which I am responsible," and "[to] design and maintain each system in a manner to support the purpose of the system to the organization." Allowing an unstable and insecure system due to unreliable software prevents the necessary integrity, which was most likely present before the update, from ensuring its prior stability. The action could also make the system unavailable or unreliable as the package has yet to be tested. Implementation would also violate the second clause, as maintaining a system includes upholding previous security measures and procedures held in place. Acting rashly and without testing or proper debugging/penetration testing does not benefit any organization and instead puts them in a vulnerable position. If, say, the company for which this package would be deployed has a policy regarding the proper internal testing of new software before deployment, but you, the recipient of the request, were unaware or were pressured without sufficient knowledge of the organization's rules, you might not even be aware of the types of risks that this

could impose, or even if those supposed risks were illicitly mentioned to you, or purposefully omitted with the instructions. Limoncelli mentions this ethical concern by stating, "Allowing employees to remain uninformed about update policies can be dangerous for business reasons. System users who do not realize what risks their actions involve cannot manage those risks". As the system administrator, you now do not know the potential risks, including any gaps or holes in the code that destabilize integrity. Completing this request ignores the blatant ethical issue of respecting system integrity.

In order to retain his trust as a system administrator, they should address the ethical concerns of deploying untested software through the use of the USENIX Code of Ethics, specifically the principles regarding communication, Privacy, and system integrity. Additionally, they should review company policy to determine if deploying the software violates any specific rules. Additionally, the system administrator should escalate the issue to higher-ups in the organization, after which the responsibility for making the final decision shifts from the system administrator to those with more authority. If time permits, the system administrator could also conduct further testing, fix bugs, and improve the stability of the software package. Which would help prevent future risks for both the system and users.

The prompt underscores the importance of using a system such as the USENIX Code of Ethics so that System Administrators can navigate ethics clearly and responsibly. This case modeled many ethical violations expected to be upheld by System Administrators, such as communication, Privacy, and system integrity, and demonstrates the potential repercussions of deploying untested software, including loss of trust, security breaches, and compromised stability. By respecting communication and addressing all possible risks, system administrators can work to protect both user trust and the interests of their company. System administrators

should view ethical considerations as a critical aspect of their work and responsibilities, utilizing frameworks like the USENIX Code of Ethics to balance their innovation with accountability.

References

- “System Administrators’ Code of Ethics.” *USENIX*, 29 Dec. 2016, www.usenix.org/system-administrators-code-ethics.
- Limoncelli, Thomas A. “Chapter 12. Ethics.” *The Practice of System and Network Administration*, Addison-Wesley Professional.