Korie Cooper

CYSE201s

4/12/2026

System Administrators

Understanding People to Manage and Protect Infrastructure

The typical person may have certain preconceived notions of what a system administrator is like. Most people think of someone primarily responsible for configuring servers, hardening networks, and troubleshooting long standing, seemingly insurmountable technical problems. From a social science perspective, however, it is often underappreciated how social based aspects of system administration do the work of system administrators. In addition to their technical tasks, they interact frequently with end users, manage expectations of higher level managers, attempt to enforce organizational security policy, and make decisions affecting users of many different systems across an organization. This is especially true in Department of Defense and Navy mission areas where system administrators are challenged to work in a high stress environment, at a fast pace, and address security needs critical to the military. When preparing for certifications like the Red Hat Certified System Administrator or the Microsoft Azure Administrator, many candidates believe that they need to understand only technical material. But technology also exists to serve Human and Organizational systems, and the tools of the Social Sciences can be surprisingly effective in helping to understand user behavior and how technology is actually used. The Social Sciences are traditionally based on several key principles like Rational choice theory, Marxian economics, cognitive dissonance, and social learning

theory. These are the same principles that System Administrators use to approach a given problem.

Rational choice theory models human behavior by taking the position that individuals decide to act in ways that maximize their self interest based upon an assessment of potential cost versus benefits. From a system administrator's perspective, understanding user behavior and the reasons behind their actions can provide some insight into security threatening actions such as bypassing security restrictions, sharing of passwords, or ignoring instructions regarding installation of software updates. A Navy system administrator is responsible for supporting users at one federal agency. He stated that his users took a path of least resistance in their efforts to complete their tasks. They followed a process that they perceived to offer them immediate benefits with minimal risk of potential problems. Security was obviously the looser in this case. Sailors and DoD civilian employees working under pressure will always select the path of least resistance or the quickest fix unless our system design dictates otherwise. By earning Red Hat certifications, system administrators will learn how to configure complex Linux/Red Hat based systems. More importantly, they will learn how to design and configure systems that make the secure path the easy path. This includes locking down systems to prevent unauthorized access, automating security updates, and enforcing appropriate permissions to prevent end users from performing incorrect and potentially hazardous tasks. The vast majority of successful cyber incidents are the result of exploiting human behavior as opposed to purely technical exploits (CISA, 2023).

Power imbalances in organizations in which those who are system administrators have a unique position of power over information systems, being able to grant or deny access to information and resources to other users at all levels of organization, including high level executives and officials who are typically above administrators in the organization's hierarchy. The particular challenges of DoD adjacent environments also face administrators. A System Administrator responsible for keeping the workstations of senior officials up and running might discover a critical vulnerability on a senior officer's workstation and be dissuaded from fixing the issue due to organisational considerations. Seen through a Marxian understanding of power, this conflict is not simply a personal one, but reflects the structure of power distribution that ultimately determines the security outcome. Preparing for the Azure Administrator certification will help IT professionals develop the skills needed to manage large scale infrastructure deployments on Azure and address real world issues related to access governance and accountability from a social as well as technical perspective.

Cognitive dissonance is the social science concept that a person tends to act in ways consistent with their self image. A system administrator, who expects to run into cognitive dissonance when a user feels that they are a good person and has done something policy breaking or caused a security incident, may find that the user denies responsibility for their actions or tries to diminish their impact. The user may even attempt to redirect responsibility for their actions. The same cognitive dissonance can be expected when a user objects to a password policy, a system upgrade, or any other administration action. A good system anticipates such dissonance and plans for the user to attempt to excuse or blame shift for their actions. Building a secure environment by default helps to eliminate many of the opportunities for users to experience

cognitive dissonance by removing the choice that they can make which would cause them discomfort. Understanding how this works can also help system administrators communicate secure practices to users in a way that eliminates much of the cognitive dissonance that the administrator's messages would otherwise generate, by structuring those messages in a way that reduces the conflict between users' perceptions of themselves and the message the administrator is trying to get across.

Observing others learn a behavior is a cornerstone of Social Learning Theory (Bandura). As a system administrator tasked with building or re establishing a healthy security culture within an organization, the same rule applies. By observing leadership be expected to follow the same security practices that are expected of the rest of the organization by HR, compliance, and other stakeholders, the organization sees significant improvements in security compliance. By making good security practices observable and expected, system administrators can begin work changing the cultural norm in Navy organizations. While technical countermeasures can prevent intrusions, it is still a senior leader with high organizational status who fails to follow procedures or has a weak password that can undo an organization's best training efforts. Senior leaders are highly attuned to their organizational status and will model behavior that they perceive to be expected of them. This is a very powerful motivator in Navy organizations. Integrating security behavior into the security model that organizational decision makers use to guide their actions can increase staff members compliance with security policies, research in the December 2010 issue of MIS Quarterly found.

System administrators in federal and military adjacent organizations also manage systems that contain information of low income individuals and families, older adults, and others with little technical experience. The data in these systems may relate to benefits, health, and financial information. By pursuing an Azure certification, the administrator must be able to manage and provide secure access to a cloud infrastructure that may contain information unrelated to the administrator him or her, but highly relevant to the individuals and communities that the administrator serves.

Conclusion

System administration is as much a social science profession as it is a technical profession. Rational choice theory can help system administrators design systems that influence users' rational choices. Marxian economics can help system administrators understand the unequal power distribution that affects a system administrator's rational choices regarding system security. Users resist having their behavior monitored and controlled due to cognitive dissonance. A strong security culture begins from the top down and is created through social learning theory. Finally, RHCSA or Microsoft Azure Administrator certification indicates an administrator has the ability to understand the social implications of systems as well as the in depth technical knowledge to administer Linux or Microsoft Azure systems.

References

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Quarterly, 34(3), 523 to 548.

Cybersecurity and Infrastructure Security Agency. (2023). Social engineering and phishing. CISA. https://www.cisa.gov

National Institute of Standards and Technology. (2020). NIST special publication 800-53: Security and privacy controls for information systems and organizations. U.S. Department of Commerce.