Why Petty IT Tyrants Are the Real Enemy of Cybersecurity, Productivity, and Innovation

John H. Batchelor
University of West Florida

Timothy R. McIlveene
University of West Florida

Dennis Barber
East Carolina University

Despite purportedly acting in the best interests of the organization, many Information Technology (IT) managers succumb to desires for control and power that result in behavior that is detrimental to employees and, ultimately, the organization as a whole. Drawing from Ashforth's seminal work on petty tyranny, we highlight the unique dynamics of IT-related tyranny, characterized by micromanagement and arbitrary control over user activities. Employing models that both illustrate petty tyranny emergence and delineate the lifecycle of IT petty tyranny, this work describes how individual predispositions and organizational factors catalyze and perpetuate tyrannical behaviors. In addition, we examine the harmful effects of IT petty tyranny on employee morale, productivity, and even organizational cybersecurity. We conclude with practical advice on how organizations can recognize and mitigate IT petty tyranny to avoid negative outcomes for employees and the organization.

Keywords: petty tyranny, information technology, petty tyranny emergence, petty tyranny lifecycle

INTRODUCTION

Despite many information technology (IT) managers' claims that they act in their organization's best interests, many of their actions result from the selfish desire to control and have power over others. In theory, IT managers are there to deal with technical issues like security (requiring VPNs) and workforce productivity (i.e., implementing and maintaining enterprise software such as SAP). But many times, actions that begin with good intentions (such as ensuring the network is free of cyber threats) grow into a tyrannical nightmare where IT managers micromanage the daily activities of users to the point that they become petty tyrants.

This idea of petty tyranny goes back probably to almost the beginning of time. In academic literature, Blake Ashforth was the first to make applying the concept to organizations a popular concept in psychology and organizational behavior (See Ashforth, 1994;1997). He defined a petty tyrant as one who "Lords his or her power over others" (Ashforth, 1994, p. 755). Anyone with even a small amount of power over another can be a petty tyrant, hence using the word “petty” as a qualifier. I remember when I waited tables in college 30 years ago. A self-appointed “head waitress” took it upon herself to enforce all the rules (even the ones she made up) and would threaten to run to the manager whenever anyone did anything she did not like. One time, she went as far as to dump out all the drinks of the entire wait staff during the middle of a shift because they were not in “approved” cups. This behavior is an example of petty tyranny many of us who waited tables in college can relate to. Still, no matter what jobs you have had, you probably remember a petty tyrant who has lorded over you at some point in your life.

PETTY TYRANNY IN IT

The Special Case of Petty Tyranny in IT and Security

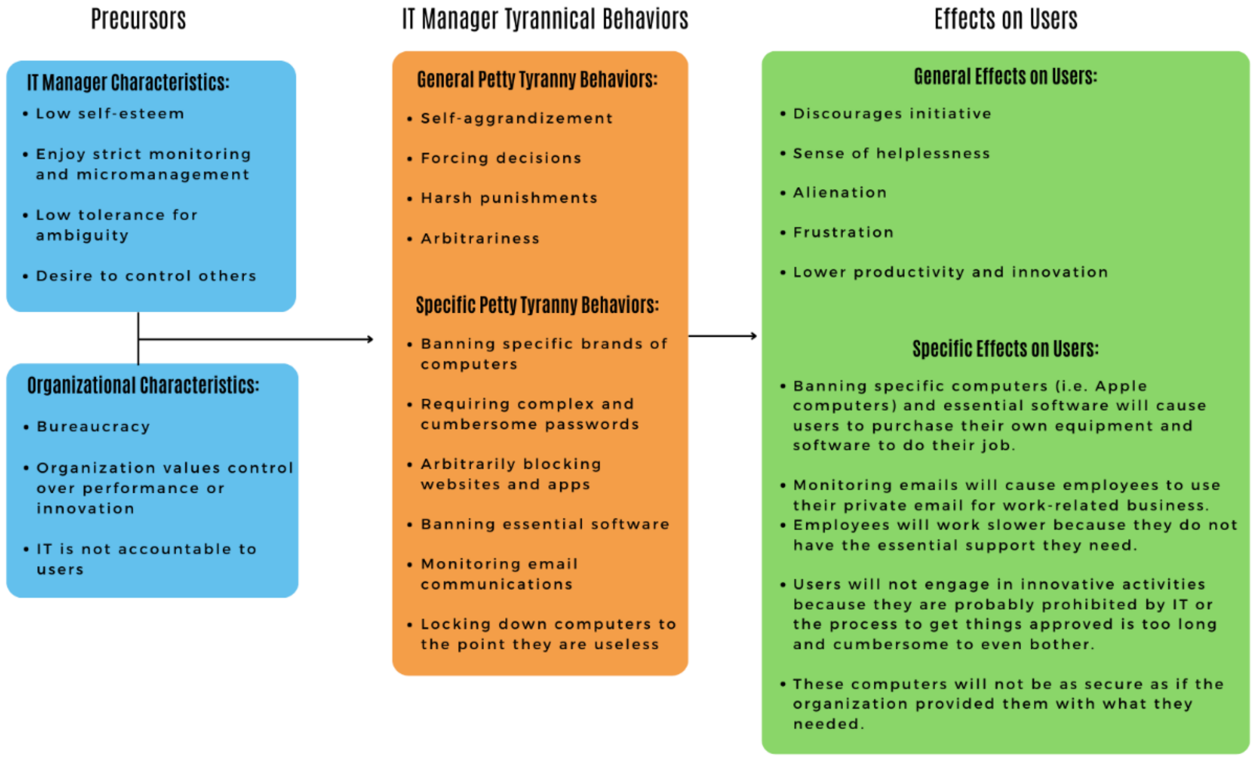
Generally speaking, petty tyrants can exist anywhere. Their behavior is characterized by arbitrariness, small-mindedness, lack of consideration for others, and forcing demands on others. In his book *Tame Your Terrible Office Tyrant*, Taylor (2009) describes such individuals as like two-year-olds (i.e., stubborn, moody, and fickle). Yet, petty information technology (IT) tyrants engage in specific behavior unique to their position as the “security” watchdog for their organizations. These people generally do not have direct line authority over others (outside of their staff) but do have staff authority (not direct supervisory authority over the user per se, but authority over their use of IT) over almost everyone in their organizations because of the nature of IT in modern business (i.e., installing and upgrading software and hardware, designing systems and programs, directing online operations, etc.). Figure 1 presents a model of such tyranny in modern organizations that misguided IT managers often inflict in the farcical name of security and best practices.

A Model of IT Petty Tyranny Emergence & Lifecycle

The emergence of petty tyranny begins with the intersection of certain IT managers and organizational characteristics (see Figure 1). We post that IT managers who are likely to engage in petty tyrannical behavior typically have low self-esteem and a low tolerance for ambiguity, which manifests as strict micromanagement and a desire to control the actions of others (i.e., requiring employees to carry their computers, laptops, and desktops, to the IT managers office once every month for inspection or refusing to communicate with workers through telephone/text/email even in emergencies, thus only communicating through work service tickets (i.e., JIRA), requiring complex forms to be filled out for simple tasks and rejecting them for minor errors). This type of behavior is enabled in organizations that are highly bureaucratic, value control over performance or innovation, and have an IT department that is not held accountable for user experience.

Theoretically, these precursors then lead to IT manager tyrannical behaviors, which are both general and specific. General tyrannical behaviors include self-aggrandizement on the part of the manager, forcing decisions on users that appear to be arbitrary, and harsh punishments for anyone who dares to violate the regime. Specifically, this tyrannical behavior is represented by banning specific brands of computers and essential software, requiring unnecessarily complex and cumbersome passwords, arbitrarily blocking websites and apps, and monitoring email communications. Examples include requiring someone to reset their password because the IT manager is mad at them, banning specific brands of computers and software because the IT manager is not proficient at working on them, requiring administrative approval for access to commonly used instructional websites (such as the Purdue Owl) to show workers who is in control, and intentionally taking months to approve simple things like updating software that the organization already approves. In effect, this behavior renders the user’s computer practically useless for completing their job-related tasks.

FIGURE 1
PETTY TYRANT EMERGENCE


Precursors
IT Manager Tyrannical Behaviors
Effects on Users
IT Manager Characteristics:
• Low self-esteem
• Enjoy strict monitoring and micromanagement
• Low tolerance for ambiguity
• Desire to control others
Organizational Characteristics:
• Bureaucracy
• Organization values control over performance or innovation
• IT is not accountable to users
General Petty Tyranny Behaviors:
• Self-aggrandizement
• Forcing decisions
• Harsh punishments
• Arbitrariness
Specific Petty Tyranny Behaviors:
• Banning specific brands of computers
• Requiring complex and cumbersome passwords
• Arbitrarily blocking websites and apps
• Banning essential software
• Monitoring email communications
• Locking down computers to the point they are useless
General Effects on Users:
• Discourages initiative
• Sense of helplessness
• Alienation
• Frustration
• Lower productivity and innovation
Specific Effects on Users:
• Banning specific computers (i.e. Apple computers) and essential software will cause users to purchase their own equipment and software to do their job.
• Monitoring emails will cause employees to use their private email for work-related business.
• Employees will work slower because they do not have the essential support they need.
• Users will not engage in innovative activities because they are probably prohibited by IT or the process to get things approved is too long and cumbersome to even bother.
• These computers will not be as secure as if the organization provided them with what they needed.

These negative behaviors on the part of the IT manager then impact users, which, ironically, are the employees they are tasked with supporting to enable success. Effects on users from petty tyrannical behavior on the part of IT managers are also general and specific. Generally, the impacts on users include experiencing decreased initiative, a sense of helplessness, frustration, lower productivity, and lower continuance commitment (Honer & Burchell, 2022). Specifically, actions like banning certain brands of computers (i.e., Apple) or software will cause users to purchase their own equipment and software to do their jobs, which is a negative employee experience (both financially and emotionally). Although many organizations have policies against using personal equipment and software, petty tyrants force workers to choose to be less productive and possibly lose their jobs or go against such policies to perform their jobs successfully.

An example would be for a worker to use their personal software to prepare an analysis and then write the report using the approved software based on the analysis performed outside the network. Wilson et al. (2022) argues that toxic behaviors (i.e., petty tyranny) lead to insiders engaging in threat behaviors such as these actions. The workers could cover their tracks by running a similar report within the network, thus leaving a trail that would make it look like the information was processed according to approved policies. Or, if the necessary IT tools are not in place, employees will work slower and be less productive as workarounds are devised.

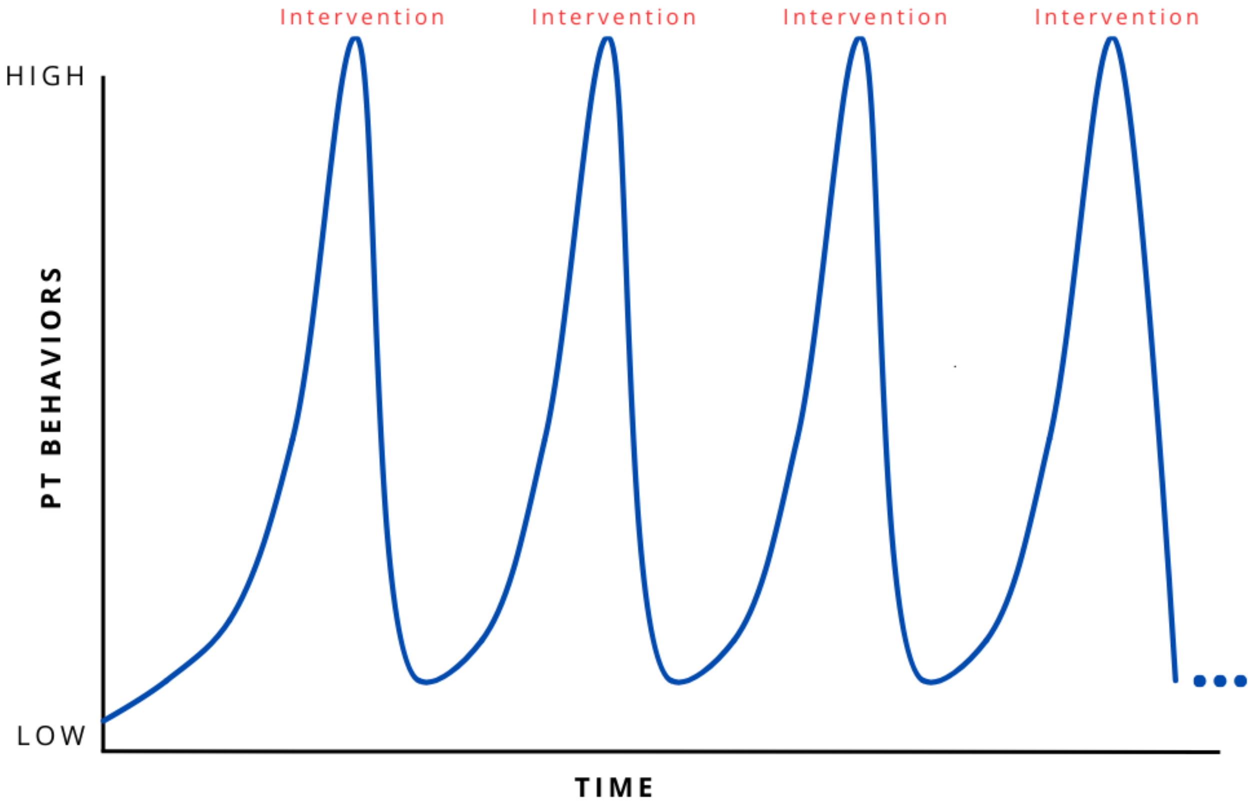
In the employee's mind, this is what their organization wants them to do; otherwise, they would not take away the necessary tools to perform their jobs effectively. In addition, by going around the IT department, workers engage in "shadow security", which lessens organizational security as these machines and programs generally do not have all the protections in place like corporate-managed assets. For instance, the work completed on personal devices will be saved outside the organization's network, making it more accessible to nefarious individuals (Kirlappos et al., 2014).

We have also developed a model to illustrate the IT petty tyranny lifecycle (see Figure 2). This figure charts the relationship between petty tyranny (PT) behaviors and interventions over time. Petty tyranny behaviors tend to grow over time as these managers constantly push the boundaries of their authority and are unimpeded by managerial oversight. However, at a certain point, these behaviors become untenable for both employees and, ultimately, the organization, which requires an intervention by management. This intervention, in the form of informal or formal reprimands or the development and communication of clearer organizational policies, reduces the petty behavior until the cycle repeats.

Thus, when the wrong personality types are hired as IT managers (i.e., low self-esteem and high desire to control others), managerial interventions only work if the petty tyrant knows they are being closely monitored. Once the monitoring ends, they slowly return to their PT baseline. For example, an IT manager may quit responding directly to the workers they serve (via email, texts, office phone, etc.) and create a complex system of using work tickets (who they get to when they feel like it) for even very simple and sometimes urgent problems (i.e., a projector is not working in a conference room where a very important customer is waiting to see a sales presentation).

This behavior may result in a managerial intervention that changes the IT manager's behavior for a short time. But until the situational factors (i.e., the IT manager still has the authority to limit access to the IT department for even urgent matters) are removed that allow this counterproductive behavior and new organizational norms are established, the behavior will continue (See Ashforth, 1994). Sarley and Renaud (2023) present a similar model of how negative employee treatment, as described herein, leads to either a virtuous or vicious cycle of employee and organizational outcomes related to cybersecurity. Thus, organizations can take action to control IT petty tyranny to create virtuous cycles that benefit the organization and employees or do nothing which will result in the opposite outcomes.

FIGURE 2
PETTY TYRANY BEHAVIORS OVER TIME



What Is a Petty Tyrant, and Why Is It a Problem in the Workplace, Especially in IT Security?

As defined by Ashforth (1994:1997), a petty tyrant is characterized as someone who utilizes even the most minuscule amount of authority or power in an attempt to control the behaviors of others simply because they can. No doubt anyone who has worked in an organization has encountered and endured multiple versions of this archetype. Beyond just the annoyance of working with a petty tyrant, this behavior creates problems in the organization that lead to negative outcomes. We believe this is especially true when petty tyrants are allowed to run rampant in the organization's IT department.

Petty tyrannical behavior by IT security personnel stems from a combination of multiple factors. First, petty tyrants develop when IT personnel lack (or simply do not care) about the business's and its employees' needs, nor do they understand the importance of social capital in employee cybersecurity participation (Fisk et al., 2023). Their decisions are framed around control and making their job easier rather than supporting or enabling the success of their "customers" (i.e., users of the company's IT systems).

Second, this behavior can develop when individuals are insecure or have feelings of inadequacy relating to their position, skill set, personal lives, or career trajectory. Third, petty tyrants have an innate desire to control the behavior of others, which is channeled through IT policies and decision-making. In some instances, this is such an engrained subconscious desire that they are unaware of the motivation behind their behaviors. Fourth, and perhaps the most significant factor in the development of petty tyrants, is the lack of management oversight and accountability that act as a hothouse that allows this behavior to flourish and take root. Many managers know very little about IT and acquiesce to the demands of their IT managers. Likely, they do not want to anger the petty tyrant themselves for fear of reprisals, such as the petty tyrant intentionally creating problems when their advice is not followed.

Examples of Petty Tyrannical Behavior by IT Security People

Examples of IT petty tyrannical behavior is legion and include banning specific brands of computers or other devices that users need to fulfill their duties. IT petty tyrants appear to enjoy banning Apple computers from the corporate network on the grounds of "security" despite the fact these machines are mainstream and enjoy a large user base. Many times, the dictates of IT petty tyrants are to cover up for their inadequacies. For example, I know one IT manager who banned Apple computers because he was not good at working on them. Thus, instead of undergoing additional training to improve at his job (and admitting he did not know something due to his low self-esteem), he banned Apple computers for everyone in the name of "security."

Another issue is requiring employees to use complex and cumbersome passwords that must be changed frequently and beyond the normal security protocol or lack of evidence of a security breach. This type of IT tyranny can be counterproductive. For example, corporate password requirement regimes can be so strict and narrow as to be extremely difficult to formulate and remember. As a result, employees may keep their passwords on a note on their desk as a workaround, thus likely making the system less secure than if less dictatorial password protocols were in place (Alotaibi et al., 2016).

Other examples include blocking websites and applications deemed, in the eyes of the IT petty tyrant, not essential for the user's work function but can be used to increase organizational productivity (Linzon, 2020). Many companies block employee access to video streaming sites like YouTube that could serve a legitimate business purpose regarding supplementing employee training. Finally, micromanaging employee work habits, internet activity, and email communications are other classic IT petty tyrannies despite violating organizational policies.

The Negative Consequences of Petty Tyrannical Behavior by IT Security People

When IT departments allow petty tyrants to run rampant, the organization experiences negative consequences and outcomes. Organizations are more likely now than ever to ignore such behaviors because of the shortage of IT professionals. The workforce skill gap for cybersecurity employees is a serious problem in the United States and internationally (Schaeffer et al., 2017). Cameron and Marcum (2019) note that this shortage of cybersecurity talent will likely worsen over time. Thus, this article is more relevant now than ever because organizations need not lose sight of the importance of hiring the right type of IT staff in the mad dash to fill employment gaps.

It is important to note previous research (Bateman & Organ, 1983) has established that employees view organizational authority figures as a proxy for the broader organization. Therefore, when subjected to petty tyranny from the IT department, which has authority over usage policies, the employee's relationship with the broader organization is damaged. Employee commitment to the organization is lowered, resulting in decreased morale, lower productivity, and increased turnover rates. The company's innovation ability is stymied as employees either leave or throw their hands up in frustration. This lack of innovation leads to poor performance and damage to the company's reputation. Perhaps the most perverse outcome of petty IT tyrannies is the increased risk of security breaches. Employees utilize workarounds and other shortcuts to avoid being subjected to the whims of the IT department, which often means bypassing necessary security procedures.

How to Prevent IT Security People From Becoming Petty Tyrants

To avoid these negative outcomes, organizations must be proactive to prevent IT security personnel from becoming petty tyrants. Prevention is the best way to combat petty IT tyrants in organizations. Hence, proper pre-employment screening is essential. Before hiring IT managers, candidates should undergo personality evaluations or be interviewed in a way that looks for warning signs such as low self-esteem, low tolerance for ambiguity, and an overbearing/ controlling disposition.

For existing IT managers, providing training in the business's and its employees' needs is a great place to start. This would be perspective training, where IT managers are forced into situations where they are exposed to extreme micromanagement and petty attacks and then must reflect on how these practices made them feel, thus forcing them to reflect on how their actions affect others. When IT understands its role in the context of the greater organization and its mission, IT employee energy and mindshare can be channeled into ways of supporting success rather than inflicting unnecessary misery on others. Next, organizations would be well served to create a culture of trust and respect between IT security and other departments. It is much more difficult to engage in tyrannical behavior when you have a positive relationship with the intended recipients.

From a practical standpoint, organizations must establish clear and concise security policies and procedures that create boundaries for IT actions. An example would be having a rapid appeal process (to a non-IT manager to act as an arbitrator) for IT-related decisions. In conjunction, organizations must hold security people accountable for their actions. When policies are violated via petty tyrannies (i.e., the improper monitoring of employee email, internet usage, etc.), the organization has a responsibility and duty to stop this behavior before it is allowed to take hold and impact performance. Finally, organizations should provide IT security personnel opportunities to grow and develop their skill sets for their betterment and the organization's. Focusing on growth reduces the temptation to engage in petty tyrannical behavior.

CONCLUSION

The harsh reality is that certain people are attracted to certain jobs. When managing IT, there is a lot of bait (i.e., staff authority over many people with few checks and balances) attracting petty tyrants. Organizations need to be aware of this and adjust accordingly. When hiring IT managers, organizations must screen for the negative personality traits and predispositions listed herein. In addition, screening for positive personality traits in soft skill areas like communication, problem-solving, understanding, and teamwork is critical (*Soft Skills Training Boosts Productivity, 207*; Cacciolatti et al., 2017). Research has found that workers who had received training on developing good soft skills were 12% more productive than workers who had not (*Soft Skills Training Boosts Productivity*, 2019). For existing IT managers, close supervision of overreach and micromanagement is key. Organizations cannot allow the fear of reprisals and sabotage from IT managers to prevent them from ensuring that a single IT manager's rogue actions do not hamper performance and innovation for the entire organization.

REFERENCES

Alotaibi, M., Furnell, S., & Clarke, N. (2016, December). Information security policies: A review of challenges and influencing factors. In *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)* (pp. 352–358). IEEE.

Ashforth, B.E. (1994). Petty tyranny in organizations. *Human Relations*, *47*(7), 755–778.

Ashforth, B.E. (1997). Petty tyranny in organizations: A preliminary examination of antecedents and consequences. *Canadian Journal of Administrative Sciences*, *14*(2), 126–140.

Bateman, T.S., & Organ, D.W. (1983). Job satisfaction and the good soldier: The relationship between affect and employee "citizenship." *Academy of Management Journal*, *26*(4), 587–595.

Cacciolatti, L., Lee, S.H., & Molinero, C.M. (2017). Clashing institutional interests in skills between government and industry: An analysis of demand for technical and soft skills of graduates in the UK. *Technological Forecasting and Social Change*, *119*, 139–153.

Cameron, E.A., & Marcum, T.M. (2019, March 27–29). *Why business schools must incorporate cybersecurity into the business curriculum – Preparing the next generation for success*. Chicago, IL, United States: Society for the Advancement of Information Systems.

Fist, N., Kelly, N.M., & Liebrock, L. (2023). Cybersecurity communities of practice: Strategies for creating gateways to participation. *Computers & Security*, *132*, 1–11.

Kirlappos, I., Parkin, S., & Sasse, M.A. (2014). Learning from "Shadow Security". In *NDSS Workshop on Usable Security*.

Lindzon, J. (2020, January 24). *Does blocking certain websites at work hurt employee productivity?* Fast Company. Retrieved from https://www.fastcompany.com/90453980/does-blocking-certain-websites-at-work-hurt-employee-productivity

Schaeffer, D.M. (2017). An interdisciplinary approach to cybersecurity curriculum. *Journal of Higher Education Theory and Practice*, *17*(9), 36–40.

Searle, R., & Renaud, K. (2023). *Trust and vulnerability in the cybersecurity context*. Hawaiian International Conference on System Science, Lahaina, HI, United States.

Taylor, L. (2009). *Tame your terrible office tyrant*. Wiley.

University of Michigan News. (2019, May 28). *Soft skills training boosts productivity*. Retrieved from https://news.umich.edu/soft-skills-training-boosts-productivity/

Wilson, G., Wolford, R., Beneda, J., Ellis, S.K., & Laros, S.L. (2022). *Better ways to work together: A playbook for understanding and changing toxic workplaces*. The Threat Lab.