**EMCS2600: The Future of Cybersecurity: Technology and Policy**

Assignment: 2nd Short Response Paper for Modules 4-5

Brian Russel Davis, [brian\_davis@brown.edu](mailto:brian_davis@brown.edu)

*Assume that you have been hired as a CISO. Your organization and its computing infrastructure are growing. Explain and defend the long-term objectives you set for modifying the infrastructure as it grows so as to improve security while keeping costs under control.*

#### Note

My paper takes what may be a controversial stance on white privilege and the way it affects decision making in the enterprise, more specifically an organization’s long term security objectives. It’s not a common argument, only because of the invisible prevalence of white privilege and the discomfort this discussion causes for white people. However, since these types of constructs do not simply decay on their own, it is the job of people like me to bring the issues into focus so it can be confronted and dismantled. In **every** company I have worked in for the last 21 years I have witnessed the misuse of resources that stem from the prevalence of toxic privilege even though it violates written and widely accepted internal rules and norms.

#### Introduction

Growth in an organization can mean several different things including more users, more locations, more employees, more traffic/usage or a combination of some or all of these. Growth in any of these areas can change the security posture of an organization dramatically even though many of the profound changes may go unnoticed. The infrastructure, which I will argue is the main instrument for communication among the users and resources in the enterprise, will need to accommodate growth while maintaining the ability to monitor, detect and respond to internal and external threats. However, the infrastructure will become ineffective and useless unless companies align their long term objectives with strong principles of inclusion that dismantle the more toxic elements of white privilege and white supremacy that have been present in American life since the 1400s. Ignoring the issue and allowing privilege to break the security and integrity of the infrastructure is preventable and better yet, the protections can be automated.

#### Example

Adam Neumann, the founder of WeWork, is the latest example of white privilege running amuck. In the course of just a year, he single-handedly turned a company with a valuation of 47 billion dollars ( the second-highest among start-ups ) into an 8 billion-dollar company with a deeply scarred reputation. With no one to check his power, he ran roughshod over his investors, users, and employees as he broke norms, laws and ran WeWork as a personal project. The most surprising part of the WeWork story is not what Adam did but it's the corporate structure that would allow it. WeWork's failure is not unique or uncommon. In fact, almost all of the organizations that I have worked for were run by a person like Neumann. The same toxic environment engulfed Uber, Facebook, Twitter, and countless others. Toxic leadership undermines planning, communication, and organizational consistency. All of this dysfunction opens a gap for attackers and robs the organization of it's most precious asset, input from a diverse set of users and employees.

#### Problem v Solution

How can organizations maintain transparency and accountability without a strong commitment to fairness and honesty at the very top? Furthermore, how can any organizations build infrastructure with meaningful objectives when leadership lives above the rules? When we look closely at security failures, the really big ones, there is usually a failure in communication which was facilitated by a failure in leadership. When long term objectives are aligned with strong ethical principles, that alignment creates a strong synergy that resonates from the top, into the tools and throughout every decision made by the organization. I am going to step through three of these objectives and demonstrate how their alignment with ethical principles makes the infrastructure more effective, more cost-efficient and safeguards the organization from toxic behavior that has its roots in white privilege.

#### **Long Term Objective**: Communication is monitored equally and programmatically

Monitoring activity in the infrastructure is the first element of effective security. Without visibility and knowledge of the devices on the network and the data that is traveling between those devices, there would be no effective detection. Monitoring everything creates a big data problem, a privacy problem and an automation problem. However, setting a long term objective that is aligned with ethical principles will help narrow the scope of the problem. Most organizations, especially the small to medium-sized ones tend to give business leadership inappropriate access and ownership to all of the organization's resources based on their role as “the boss.” This problematic boss/owner position is a lingering artifact of white supremacy from the days of slavery where the overseer ( who sometimes doubled as the plantation owner ) executed all the responsibility and authority of the plantation including the people who live there.[[1]](#footnote-0) In the modern infrastructure we replace the overseer with AI that treats all users, activity and communication equally.

##### Strategic

Because of a managerial model that is derived from white privilege, users with leadership positions tend to bend the rules in regards to sharing sensitive information over inappropriate channels making their communications a target for attackers. By programmatically and equally monitoring the activity of all accounts, we remove the incentive for attackers to penetrate accounts held by leaders.

##### Tactical

* Programmatic monitoring and analysis should be smart enough to block and remove sensitive content before it is transmitted over an insecure channel and warn the user about the risks of the behavior.
* Programmatic monitoring and analysis should have a 200% scale capacity, and once the current capacity routinely hits 75% it should be refactored.

##### Ethical

No special privilege for people in leadership or connected to leadership when it comes to rules about how to transmit sensitive information.

#### **Long Term Objective** : Administrative access to production assets should be restricted on a need to know basis equally and programmatically.

Access to user information usually represents the crown jewels to a “would be” attacker. Just like monitoring, access control represents one of the primary functions of the security team and the infrastructure tools we use to define and regulate access. Also similar to monitoring, people in leadership are often granted unnecessary direct access to user information, again following after a toxic owner-manager model developed in the early 1400s. The truth is that only users own their data, and organizations that provide services or products are in service to the users, not the other way around. A user should be prompted to grant consent whenever the data is access or used by another human being, directly or indirectly. Laws like GDPR have created a starting point for this type of approach but organizations must adopt internal practices and growth plans that make this type of objective an ongoing actuality.

##### Strategic

Attackers often take advantage of user’s credentials that have too much access, power or permissions. By eliminating inappropriate ownership and access based on “who’s the boss”, credentials of managers or supervisors will not be conveted as targets for attackers.

##### Tactical

* Only approved applications ( not admins ) should have access to user data and no one application should have access to live user information.
* Programatic alerts should be configured to report to the user when their data has been access by another human, no matter who that human is.

##### Ethical

No special privilege for people in leadership or connected to leadership in terms of access to user data. User’s data belongs to the user and the infrastruture should be built to enforce that.

#### **Long Term Objective** : Contractors and vendors whose software or services is used to support the infrastructure should be evaluated by a diverse set of employees.

Attackers are looking for weak points in the infrastructure irrespective of who made or owns the software that contains the weakness. When an organization buys software or services from a 3rd party they are not just buying the software as it exists now but they are also buying the future updates, patches, features and potential vulnerabilities. A contractor or vendor that does not have a strong security practice can therfore create security problems for the organization. In the traditional business structure inherited from systems used to enforce white supremacy, decision making for purchasing is consolidated in the owner-manager role. This weakens the organization’s visibility into the impact of the decision on the diverse teams in within the organization, diminishes the input of people in the organization that may be best qualified to evaluate the descision and leaves no protection for an organization whose owner-manager is compromised or not working in the best interest of the business and the users.

##### Strategic

Distributing the decision making power into teams or councils removes the unecessary reliance on the intellect and wisdom of one person and enpowers people who may otherwise to

##### Tactical

* Create financial independent employe-led councils for major purchases. Each council should be formed from scratch each time a decision is needed and must record detailed notes on the decision making process for comsumption by future related councils.

##### Ethical

No special privilege for people in leadership or connected to leadership in terms of financial or purchasing decisions. The decision to spend money should not rest with one person, but should instead rest in the hands of the people most knowledgable in the target area of the purchase.

#### Conclusion

It is no wonder that we don’t hear many discussion on the need to dismantle institutions of white supremacy since its survival depends on its ability to remain invisible. The irony is that its exploitative properties make organizations that subscribe to its tenants easy targets. Consolidating ownership and access in the hands of one person or a small handful of people is just irrational and idiotic. It would be like roof that is held up by a single beam; Easily found and easily toppled.

#### Bibliography

McIntosh, Peggy. "White privilege: Unpacking the invisible knapsack." (1988).

Doane, Ashley W., and Eduardo Bonilla-Silva, eds. White out: The continuing significance of racism. Psychology Press, 2003.

Campbell, Douglas G. "“White Privilege”: A Shield against Reason." Academic Questions 23.4 (2010): 497-504.

Sobre-Denton, Miriam Shoshana. "Stories from the cage: Autoethnographic sensemaking of workplace bullying, gender discrimination, and white privilege." Journal of Contemporary Ethnography 41.2 (2012): 220-250.

1. Richter:, William L. (August 20, 2009). "Overseers". The A to Z of the Old South. The A to Z Guide Series. 51. Lanham, Maryland: Scarecrow Press (published 2009). p. 258. ISBN 9780810870000. [↑](#footnote-ref-0)