execution vulnerabilities (which was found to have the highest impact) could be mitigated by the removal of administrator rights – the message is clear: Removal and protection of administrative rights is an essential cybersecurity strategy against today's threats [2].

We have found that the SNAP approach is an effective and efficient way to increase protection of administrative accounts. By protecting against inadvertent privileged credential loss it mitigates the risk of attackers gaining system-wide access to an organizations infrastructure. Due to its simple and low-cost implementation SNAP can fix multiple security exposures that organizations must face on a daily basis. We have demonstrated how SNAP can effectively defend against several attack vectors including keyloggers, shoulder surfing, Mimikatz and forensic analysis. We have also shown how this approach can enhance incident response in both attempted, and actual breach investigations. We believe that with appropriate training and enforced adoption, system administrators can use this method to better secure their privileged access and in turn the infrastructure for which they are responsible.

8. Acknowledgements

The authors wish to thank BYU's Office of Information Technology for their support of the Red Team and development of ideas in support of this paper.

9. References

[1] A. Wesley, *the practice of system and network administration 2nd edition*, 2nd ed. Boston, MA: Addison-Wesley, 2007.

[2] Avecto, "2013 Microsoft Vulnerabilities Study : Mitigating Risk by Removing User Privileges," 2013.

[3] D. Ferraiolo, J. Cugini, and D. R. Kuhn, "Role-based access control (RBAC): Features and motivations," *Proceedings of 11th annual computer security application conference*. pp. 241–248, 1995.

[4] R. Sandhu, D. Ferraiolo, and R. Kuhn, "The NIST model for role-based access control," *Proc. fifth ACM Work. Role-based access Control - RBAC '00*, pp. 47–63, 2000.

[5] E. Bertino, P. A. Bonatti, and E. Ferrari, "TRBAC: A temporal role-based access control model," *ACM Trans. Inf. Syst. Secur.*, vol. 4, no. 3, pp. 191–233, 2001.

[6] "What Network and Computer Systems Administrators Do," *Bureau of Labor Statistics*, 2014. .

[7] "What is an administrator account?," *Microsoft*, 2015. .

[8] "Pre-built administrator roles," *Google*, 2015. .

[9] H. Setty, "System Administrator - Security Best Practices," *SANS Inst. InfoSec Read. Room*, no. May, 2001.

[10] D. R. Lindemann, "The Evolution of Authentication," *FIDO Alliance*, 2013.

[11] S. Moses, J. Mercado, D. Rowe, and A. Larson, "Touch Interfaces and Keylogging Malware," in *Proceedings of the 11th International Conference on Innovations in Information Technology (IIT'15)*, 2015.

[12] C. a Wood and R. K. Raj, "Keyloggers in Cybersecurity Education," 2015.

[13] M. Allen, "Social Engineering - A Means to Violate a Computer System," *SANS Inst. InfoSec Read. Room*, 2007.

[14] S. Duckwall and C. Campbell, "Hello my name is Microsoft and I have a credential problem," in *BlackHat 2013*, 2013.

[15] M. Little, "Password Security: A Case History by Rober Morris and Ken Thompson (Bell Labs)," 2004.