

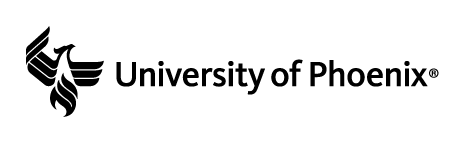
Security Assessment Report (sar)



August 3, 2020

SHANE ẼIRE BYRNE

CYB407



Week 4 – Assignment Template

**Security Assessment Report (SAR)**

Complete the table below to create a 1-to 2-page Security Assessment Report.

| **Report the Vulnerability Title and Description** | **Likelihood** | **Impact** | **Overall Risk Level** | **Recommended Mitigation** |
| --- | --- | --- | --- | --- |
| Social Engineering: This being a means by which a threat agent employs deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes. | Very High | Very High (This is dependent on the success of the attack, but the logical assumption is very high if the threat agent capitalized on the weakness) | Very High (Score value of 96-100) | Establishment of awareness and training for personnel; establishment of employee cyber security awareness training. Email virus detection tools (checks e-mail attachments). Proper establishment of known tactics (such as the use as phycological triggers; exempli gratia: The Nigerian Prince scheme). Establish policies to test the effectiveness of training staff. Apply technical safeguards such as firewalls, antivirus, anti-malware, whitelisting, and spam filters. Ensure all system assets are appropriately patched and thoroughly tested. |
| Unpatched Software: Known vulnerabilities in a program or code that an organization is aware of and will not or cannot fix. | Medium | High-Very High | High to Very High (score of 80-100) | Establishment of the use of auditing tools, these will help in identifying missed patches and vulnerable systems. Deployment of systemic updates to eliminate application vulnerabilities in system endpoints. Automation of the patch management process which will help to ensure the operating systems and third-party applications are patched in a timely manner. Establish policies that control when and where patches are applied. |
| Firewall Misconfiguration: An inherit flaw in the governing rules a firewall addresses system traffic through its analysis of packet filtering, applications, or packet inspection. | Low-Medium | Medium to Very-High | High to Very High (score of 80-100) | Establishment of firewall configuration guidelines. The inclusion of automated firewall systems removes the possibility of misconfiguration due to human error. Firewall automation helps to eliminate friction between DevOps and SecOps as well as increase security agility. |

References

Dosal, E. (February 14, 2020) Top 9 Cybersecurity Threats and Vulnerabilities

Retrieved from <https://www.compuquip.com/blog/top-5-cybersecurity-threats-and-vulnerabilities>

Ford, N. (31 August 2018) 5 ways to mitigate social engineering attacks

Retrieved from <https://www.grcelearning.com/blog/5-ways-to-mitigate-social-engineering-attacks>

Lord, N. (Tuesday September 11, 2018) What is NIST SP800-53? Definition and Tips for NIST SP800-50

Compliance Retrieved from <https://digitalguardian.com/blog/what-nist-sp-800-53-definition-and-tips-nist-sp-800-53-compliance>

Moshiri, M. (February 9, 2016) Securing the Unpatchable: How to Prevent Security Breaches When You Cannon Patch

Retrieved from

<https://blog.paloaltonetworks.com/2016/02/securing-the-unpatchable-how-to-prevent-security-breaches-when-you-cannot-patch/>

National Institute of Standards and Technology (NIST) (September 2012) Guide for Conducting Risk Assessments

Retrieved from <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>

Rogers, B. E., Dunkerley, D. (2015). CRISC Certified in Risk and Information Systems Control All-in-One Exam Guide.

[[VitalSource Bookshelf version]]. Retrieved from vbk://1260118088 is

SolarWinds (08-23-2013) Mitigating The Risks Of Unpatched Applications!

Retrieved from <https://thwack.solarwinds.com/t5/Geek-Speak-Blogs/Mitigating-the-Risks-of-Unpatched-Applications/ba-p/441578>

StorageCraft Technology Corporation (January 17, 2020) Is Unpatched Software a Security Risk Retrieved from

https://blog.storagecraft.com/unpatched-software/#:~:text=Unpatched%20software%20means%20there%20are,for%20and%20perform%20regular%20updates.

Whitney, L. (November 12, 2019) How firewall automation can help prevent breaches caused by wrong configurations

Retrieved from

<https://www.techrepublic.com/article/how-firewall-automation-can-help-prevent-breaches-caused-by-wrong-configurations/>

Wickert, Kyle (09/17/2015) 5 Most Common Firewall Configuration Mistakes

Retrieved from <https://www.darkreading.com/operations/5-most-common-firewall-configuration-mistakes-/a/d-id/1322225>