

Walmart--Risk Management Framework Whitepaper

Module 1 Assignment

Eric Wendt, CEO of Pink Robot Security

CSOL 530

***Introduction***

As the world’s largest brick and mortar retailer, Walmart is exposed to serious and relentless threats from cyber-criminals. This threat exposure will only increase as Walmart increases its online presence and makes a bid to challenge Amazon in e-commerce. Although only a small percentage of Walmart’s 450 billion dollars in worldwide annual sales are from online transactions, that percentage is growing. And as this share of sales grow, so will the risks. In this whitepaper, we hope to discuss some of these risks, the importance of a cybersecurity risk management framework in securing against these risks, and what Pink Robot can do to help.

***Areas of Vulnerability***

Before we discuss the development of a risk management framework for Walmart’s ecommerce branch, let’s clearly establish why such a framework is important by defining some common threats. Some of these threats, like SQL Injection, might engender fear merely by their cryptic sounding names, just as a disease like Necrotizing fasciitis sounds like something we want to avoid even before we know what the name means. Other threats, like malware, may sound so familiar and banal that we might fail to take them as seriously as we should. Some common threats, or areas of vulnerability, include:

***SQL Injection***—According to OWASP, SQL injection consists of “the insertion or ‘injection’ of a SQL query via the input data from the client to the application” (OWASP, 2016). Practically speaking, this could mean an attacker exploiting a vulnerability in a Walmart web application to “inject” a query and get back information from the backend database. This information could include confidential customer financial information.

***Cross-Site Scripting (XSS)***—Cross-Site Scripting is a type of injection where an attacker sends malicious code, often in the form of a browser side script, to an end user of the application, who unsuspectingly trusts and executes the script, allowing the attacker to access “cookies, session tokens, or other sensitive information retained by the browser” (OWASP, 2018).

***Parameter Tampering****—* Parameter Tampering is another method of entering data, such as a new price for an item, into the browser. A web application whose server has weak “data sanitization” is vulnerable to such attacks (Skrupsky, Bisht, Hinrichs, Venkatakrishnan, & Zuck)**.**

***Malware—***Malware is short for “malicious software” and encompasses a broad spectrum of threats from viruses, to worms sent via phishing emails, to spyware, and is generally meant infect a user’s computers or devices and cause harm in some way (Kapersky Lab, 2018).

Other threats and vulnerabilities include Unprotected Access Control, Remote Command Execution, Cross-site request forgery (CSRF) and more (Hampton, 2012). We cannot discuss all of the almost innumerable ways that hackers can exploit vulnerabilities in a web application, but these are some of the most common methods of attack.

***Elements of a Risk Management Plan***

Now we turn our attention to the elements of a Risk Management Plan, and how such as plan can help protect against the above-mentioned vulnerabilities. The NIST Risk Management Framework consists of five core elements: Identify, Protect, Detect, Respond, Recover. (NIST, 2014).

***Identify***—At this step we attempt to “develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities” (NIST, 2014);

***Protect***— At this step we attempt to “develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services” (NIST, 2014);

***Detect***— At this step we attempt to “develop and implement the appropriate activities to identify the occurrence of a cybersecurity event” (NIST, 2014);

***Respond***— At this step we attempt to “develop and implement the appropriate activities to take action regarding a detected cybersecurity event “(NIST, 2014); and finally,

***Recover***— At this step we attempt to “develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired die to a cybersecurity event” (NIST, 2014).

We want to emphasize that these core elements are not meant to be performed sequentially but rather concurrently and continuously as part of an ongoing risk management practice (NIST, 2014). Pink Robot specializes in the development of solid Risk Management Plans.

***The CIA Triad***

The goal of a Risk Management Framework is ultimately to protect the Confidentiality, Integrity, and Availability of data and resources (Henderson, 2017). Although most everyone is aware of what these words mean, their meaning in an information security sense is quite precise. ***Confidentiality*** is “the protection of information from unauthorized access” (Henderson, 2017). ***Integrity*** *is* maintaining the accuracy and consistency of data and only allowing authorized changes to be made (Henderson, 2017). ***Availability*** has to do withinformation being made available when and where it is needed (Henderson, 2017).

When Walmart sustains major damage against the *confidentiality* of its data, it is possible to recover, as Target demonstrated when it was attacked during the 2013 holiday season. Systems can be made more secure and confidentiality can be strengthened relatively quickly, but the damage to consumer confidence can be much more difficult to restore. Loss of consumer confidence can cost the company millions to billions of dollars in revenue. When the i*ntegrity* of data is manipulated or compromised, such as when data is manipulated or stolen in transit, the company can face even more serious problems, because if data is corrupted, systems can begin to fail. If the a*vailability* of data is compromised, this can cause systems to shut down, and consumer confidence in the robustness and security of the ecommerce web application will be damaged. None of these scenarios is good for the company, so we cannot say that damage to one part of the CIA triad is more problematic than any other part. All must be constantly maintained using a rigorous and continuous implementation of a risk management framework. In this effort, we are here to help.

# Works Cited

Hampton, T. J. (2012, September 13). *5 Security Vulnerabilities in E-Commerce Systems.* Retrieved from The HN: Web Hosting News: http://www.thehostingnews.com/5-security-vulnerabilities-in-e-commerce-systems.html

Henderson, A. (2017, March 25). *The CIA Triad: Confidentiality, Integrity, Availability.* Retrieved from Panmore Institute: http://panmore.com/the-cia-triad-confidentiality-integrity-availability

Kapersky Lab. (2018, 01 01). *What is Malware and How to Defend Against It?* Retrieved from Kapersky Lab: https://usa.kaspersky.com/resource-center/preemptive-safety/what-is-malware-and-how-to-protect-against-it

NIST. (2014, February 12). *Framework for Improving Critical Infrastructure Cybersecurity.* Retrieved from NIST: https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

OWASP. (2016, April 10). *SQL Injection.* Retrieved from OWASP: https://www.owasp.org/index.php/SQL\_Injection

OWASP. (2018, January 1). *Cross-site Scripting (XSS).* Retrieved from OWASP: https://www.owasp.org/index.php/Cross-site\_Scripting\_(XSS)

Skrupsky, N., Bisht, P., Hinrichs, T., Venkatakrishnan, V. N., & Zuck, L. (n.d.). *TamperProof: A Server-Agnostic Defense for Parameter Tampering Attacks on Web Applications.* Retrieved from University of Illinois: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.644.1193&rep=rep1&type=pdf