C768/D339 Task 1 Template

Section A: Describe Your Organization

A1: Products and Services

eBay offers a platform for independent sellers to offer a variety of products and goods to consumers worldwide.

A2: Size and Locations

Established in 1995 and headquartered in San Jose, California, with 43 office locations across 25 countries. Currently, eBay has 10 state offices in Washington, California, Oregon, Utah, Texas, and New York. The current staffing levels hover at approximately 10,800 employees.

A3: Organization’s Industry

eBay is an information technology company that provides a macro-economy for independent Sellers of a variety of goods and products.

Section B: Research Summary

Zero Trust is a security framework requiring users inside or outside the organization’s network to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data. Zero Trust assumes that there is no traditional network edge. Zero Trust addresses the modern challenges of today’s business.

B1. Source #1

ZERO TRUST SECURITY EXPLAINED: PRINCIPLES OF THE ZERO TRUST MODEL

Raina, K., 2021. What is Zero Trust Security? Principles of the Zero Trust Model. [online] crowdstrike.com. Available at: <https://www.crowdstrike.com/cybersecurity-101/zero-trust-security/>.

This article provides a high-level overview of Zero Trust in a network. It provides context into that “what” Zero Trust is, how it works, and why it is crucial for modern network security. The article then proceeds to detail how Zero Trust requires continuous vetting of access requests to provide access to resources on the network. In this tech pub, Raina provides use cases for Zero Trust to assist in protecting against Ransomware, Supply Chain attacks, and Insider threats. Raina then continues to illustrate how Zero Trust can significantly reduce the “blast radius” in the event of an internal or external breach occurs.

B2. Source #2

NIST – Zero Trust Architecture

Rose, S., Borchert, O., Mitchell, S., and Connelly, S., 2020. NIST Special Publication 800-207 - Zero Trust Architecture. [online] https://nvlpubs.nist.gov/. Available at: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf>.

In this tech publication, Rose, Borchert, Mitchell, and Connelly preset the overarching concept of Zero Trust illustrating that Zero Trust Architecture relies on the basic concept that no implicit trust is granted to assets and user accounts. This concept is similar to the “implicit deny” policy seen with next-gen firewall configurations. If it is not explicitly allowed it will default to a deny policy. The authors then go on to detail how Zero Trust Architecture moves away from the normalized security stack of the old, where the network segmentation was a prime component to protect. Zero Trust Architecture provides layers of protection to assets, services, workflows, and network accounts, rather than preventing or segmenting access to the resources on the network segment.

B3. Source #3

The Cyber Defense

Dean, E., Fonyi, S., Morrell, C., Lanham, M., & Teague, E. (2021). Toward a Zero Trust Architecture Implementation in a University Environment. The Cyber Defense Review, 6(4), 37–48. https://www.jstor.org/stable/48631305

In this journal the authors provide an insight into the background of Zero Trust Architecture, detailing the originating concept that began in 1994 in the Jericho Forum. The article then continues to develop the underlying concerns addressed by Zero Trust Architecture, such as data in transit and data leaving the network, allowing for a more secure and mobile workforce.

Section C: The White Paper

Because eBay is an Information Technology company and online retailer that strives to ensure the best experience for both employees and members Zero Trust Architecture would ensure security beyond the network edge, ensure security between on-prem and cloud data centers, and increase the trust and stability of the numerous internal and external applications used by both members and their employees.

“Zero Trust is a framework for securing infrastructure and data for today’s modern digital transformation. It uniquely addresses the modern challenges of today’s business, including securing remote workers, hybrid cloud environments, and ransomware threats. While many vendors have tried to create their definitions of Zero Trust, there are several standards from recognized organizations that can help you align Zero Trust with your organization (Raina, 2021)”. Some of the earliest formal work on what we now call Zero Trust started around in a security consortium known as the Jericho Forum, later merging into “The Open Group Security Forum” (Davis, Simos, and Skoniecki, 2020) This early concept focus on removing the “protect the perimeter or edge” of the network, instead focusing on the continued protection of the applications and data there-in.

Zero Trust Architecture is a security framework requiring all users, regardless of physical location internal or external to the organization's network to be authenticated, authorized, and continuously validated before being granted or keeping access to applications and data. Zero Trust removes the concept of the network edge, meaning regardless of end-user physical location or proximity to the local network they are scrutinized as a new connection. Zero Trust Architecture also removes the physical and logical boundaries of network edge as it operates independently between local, cloud, or hybrid network configurations. Zero Trust Architecture is designed to break down the need to protect these segmentations and allow for a more mobile workforce. Gone is the concept of protecting the network edge, and allowing users who have authenticated to that edge.

Zero Trust Architecture works to remove the concept of protecting the network edge. In a traditional network, users are authenticated to a gateway or entry point on the network commonly referred to as the “network edge” this is usually a next-generation firewall that is configured with static security policies that allow or deny access while leveraging access control lists. Zero Trust Architecture works to remove the “network edge” or “trust but verify” concepts, instead relying on the concept that “no implicit trust” will be allowed, meaning users are validated at every step of a workflow, from selling an item on the eBay site, to configuring and deploying new applications on the internal network to support internal employees supporting members. This would significantly reduce the number of credentialed attacks commonly seen with online vendors. More than 80% of all attacks involve credentials use or misuse in the network (Raina, 2021). Zero Trust would further work to prevent these credentialed attacks as if one user account is compromised the blast radius is isolated or contained to that single account as Zero Trust Architecture works to reduce an attacker’s ability to pivot or escalate privileges as they are checked and validated real-time. This is a vital step in protecting personal identifying information (PII) and payment card information (PCI). This further provides for posturing for SOC 2 and PCI compliance.

In conclusion, eBay needs Zero Trust Architecture because eBay is not only an online retailer but a very strong Information Technology company. eBay has multiple data centers, both on-prem and cloud, that support hundreds of databases and applications across a global economy. With eBay being an early developer in the IT industry they suffer from a plague of old or ad-hoc applications that are propped up by technology that was either entirely designed, built, and implemented in-house or highly adapted to the unique landscape of multiple network segmentation and physical locations. eBay could benefit from Zero Trust Architecture because they need to protect more than just the network edge, they host numerous internal and external applications and have a responsibility to protect member data in rest and motion.

Section D: Explanation of Diction

The diction is kept semi-formal as this is written for an executive audience; however, the diction is also a bit pedestrian due to the topics chosen. The executive audience will not need the intricate technical details taken to implement and maintain a Zero Trust Architecture, instead, they need to understand the “what” and “why” Zero Trust Architecture is needed.

Section E: Sources

Rose, S., Borchert, O., Mitchell, S., and Connelly, S., 2020. Zero Trust Architecture. [online] NIST. Available at: <https://www.nist.gov/publications/zero-trust-architecture>.

Rose, S., Borchert, O., Mitchell, S., and Connelly, S., 2020. NIST Special Publication 800-207 - Zero Trust Architecture. [online] https://nvlpubs.nist.gov/. Available at: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf>.

Raina, K., 2021. What is Zero Trust Security? Principles of the Zero Trust Model. [online] crowdstrike.com. Available at: <https://www.crowdstrike.com/cybersecurity-101/zero-trust-security/>.

Dean, E., Fonyi, S., Morrell, C., Lanham, M., & Teague, E. (2021). Toward a Zero Trust Architecture Implementation in a University Environment. The Cyber Defense Review, 6(4), 37–48. https://www.jstor.org/stable/48631305

Davis, J., Simos, M. and Skoniecki, J., 2020. Back to the future: What the Jericho Forum taught us about modern security - Microsoft Security Blog. [online] Microsoft Security Blog. Available at: <https://www.microsoft.com/security/blog/2020/10/28/back-to-the-future-what-the-jericho-forum-taught-us-about-modern-security/>.