Activity 1: Cybersecurity Standards and Regulations

This document is intended to guide your coursework and set expectations to enable you to fulfill the course requirements. You are expected to complete all the tasks and ensure that the objectives are met. The format of your coursework activities is guided using this template. All activities must be completed on time. It is highly recommended that you manage your time effectively throughout the term to avoid falling behind. This document is required for your portfolio submission

|  |  |
| --- | --- |
| **Objective** | **Status** |
| Topic: Equifax breach 2017  Task: Read the following article and answer questions outlined in the analysis section  URL: https://www.csoonline.com/article/567833/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html | Completed  Pending |
| **Analysis** |
| Nature of Failure:   * Was this primarily a privacy failure (e.g misuse of personal information), a security failure (e.g system vulnerability exploited), or a combination of both? * Answer: <Provide your answers in here> * I think the Equifax breach 2017 is more of a security failure. The direct cause was that attackers found and exploited technical vulnerabilities in infrastructure and internal control. Those security failures enabled the breach in the first place.   Root cause and Prevention:   * What were the main causes of the breach (technical, human, organizational, or regulatory gap)? * What measure (laws, standards, or best practices like NIST/ISO) could have prevented or minimized the impact? * <Provide your answers in here> * I think the main cause of Equifax breach comprises all options such as technical, human, organizational, and regulatory gaps. The technical cause was a failure to patch Apache Struts, which is an open-source development framework for creating enterprise Java applications that Equifax uses. Both the human and organizational causes were poor patch management because someone neglected to renew a security certificate despite having procedures in making sure patches were applied. The regulatory gap was that those handling sensitive personal information were not really enforcing cybersecurity standards. * The Equifax breach demonstrates that compliance with well-established standards like NIST CSF, NIST 800-53, and ISO 27001, combined with stricter regulatory requirements such as those found in GDPR, could have either prevented the incident or at least minimized its scope and impact. Ultimately, cybersecurity requires both robust internal practices and external regulatory enforcement to ensure that organizations handling sensitive personal data prioritize its protection.   Impact and Consequences:   * Who was affected (individuals, organizations, governments)? * What were the short-term and long-term impacts (Financial, reputational, or legal? * <Provide your answers in here> * The Equifax breach primarily harmed individuals by exposing sensitive personal data, but it also heavily impacted organizations—both Equifax itself and the broader financial ecosystem—and required government intervention at multiple levels. Its broad impact illustrates how cybersecurity failures at a single large entity can ripple across society. * In the short term, Equifax suffered immediate financial losses, reputational damage, and legal action. In the long term, it endured costly settlements, structural changes to its security operations, lasting reputational harm, and heightened regulatory scrutiny. The incident underscores that cybersecurity failures can have enduring impacts far beyond the initial breach. |