Product Safety Case Study. Paper details Instructions Objective: Critically analyze a real-world case study based on business law and ethics. Instructions Carefully review the following case study and the two scenarios presented. Be mindful that you are weighing business interests against ethical and legal obligations. Read The Vulnerability Disclosure Debate Introduction The debate over “responsible” disclosure of software vulnerabilities has been a mainstay in the security space. In 2015, new fuel was added to the fire as Google disclosed a Microsoft Windows vulnerability, along with exploit code, two days before the scheduled patch. (Exploit code is the stretch of code that hackers can exploit to hack software.) And in 2018, the debate came back into the forefront with the infamous Intel Spectre and Meltdown chip problems. The Google-Microsoft conflict highlights the issues that can arise between companies around disclosure. The Spectre and Meltdown flaws show how vulnerabilities can pit companies against the U.S. government and consumers. Company v. Company Disclosure Debate In 2015, the bug was found by Google’s in-house security research team, which searches for vulnerabilities in Google software, as well as that of other vendors, including Microsoft. Upon finding a vulnerability, Google adheres to a strict 90-day policy: Vendors are notified of the bug, and a public disclosure is automatically released 90 days after, regardless of whether the bug has been addressed. Microsoft initially asked for an extension beyond the 90 days, which was denied by Google, as was a request to extend the disclosure date to the first “Patch Tuesday” of the month (the second Tuesday of the month, and preferred release date for patches for developers). Microsoft criticized Google in a blog post, accusing the company’s decision of being a “gotcha” opportunity, and at the expense of the users, who were at risk for the two days between the disclosure and the patch release. Microsoft reiterated its support for “Coordinated Vulnerability Disclosure,” which calls for security researchers to work closely with developers in ensuring a fix is released before the public disclosure. Google, and supporters of similar disclosure policies, argue that firm disclosure dates prevent developers from sweeping vulnerabilities under the rug, and should strike a balance between the public’s right to know and providing the developer a chance to fix the problem. Many take an even harder stance and propose that immediate public disclosure is the best policy. Shortly after this incident, Google released an additional update on three Microsoft vulnerabilities. Discussion Questions What should Google and Microsoft have done differently, if anything? Did the release unnecessarily put users at risk, or is it in the best interest of users in the long run for Google to stick to its disclosure policy? Is Google’s firm, 90-day policy fair? Or should it be willing to adjust depending on the situation? Did Microsoft adequately respond? Is sticking to “patch Tuesday” enough of a reason to wait to release the patch? Should Google have published the exploit code? What obligations do security researchers have, or are they free to publish their work as they please? Companies v. US Government and the Public Disclosure Debate In 2017 and 2018, there was another high profile case of questionable vulnerability disclosure practices known as the Spectre and Meltdown chip flaws. In January of 2018, Intel revealed that millions of their computer chips were vulnerable to hacking; however, Intel did not go public with this information when they discovered it in June of 2017. Instead, Intel told select vendors about the problem (Huawei, Google, Alibaba, and Lenovo, etc.) while they worked behind the scenes to fix it. In this case, certain companies were working together to address the problem, but in July of 2018, several U.S. Senators pointed out that companies with close Chinese government ties knew about the vulnerability before the U.S. government did, putting national security and consumers’ security at risk. Discussion Questions Did Intel make the right decision to keep the Spectre and Meltdown vulnerabilities from the U.S. government and the public? Do companies have more of an ethical obligation to disclose vulnerabilities to the government and to the public than they do to direct competitors? Would immediate public disclosure of such vulnerabilities be a good best practice? Respond to the questions presented at the end of each scenarios. Submissions should be 2-4 pages in length. Submissions should contain a detailed analysis and well-thought out responses. Support your assertions regarding ethical and legal practices with credible research. You must use at least two credible sources. Court cases and federal/state statutes and regulations can be used as a credible source of information Cite and reference accordingly. All written assignments should be formatted using APA. For the current OCU APA Template, click the Student Toolkit in the top navigation bar and view the APA: Citation and Formatting Help page.