Software Reliability Individual or Team Responsibility?

Products are only as good as how they are used and maintained. A car for instance can be a great product; but, if you do not maintain it (change the oil, replace gasoline, etc.) then the product will become unreliable overtime. This is a similar situation for software (which is a product in this case), you must be vigilant and maintain it with updates, if you do not then the reliability of the service will downgrade.

The word reliability is an interesting term I believe I have heard my entire life about human produced products. "Buy American," they would say, "our products are more reliable than other countries". The problem with products and their reliability is how to determine who is at fault when the consistency of the item is less than what was advertised. Is it the engineers who drew the plans, the plant who physically produced the product, the company who paid the engineers and the producers of the product, the consumer on how the product was used, or is it everyone's fault? Personally, I think it is all situationally dependent on whose shoulders the fault falls upon. Below is an actual event I witnessed fro a case study.

I interned for this company a couple of years ago and was able to observe a particular company go through a meltdown when the software they were using was exploited by a virus. In the final write up, the computer forensics technicians wrote that the virus was used on their windows 7 servers to copy and send data to an unknown IP address (probably a hacker server). The virus got within the system by an insider opening a PDF attachment through a fishing email. The malicious program was an older virus that most anti-virus software would have identified. The software was not properly updated in a timely manner and there were no backups (because it went unnoticed the backup disks were in a failure state for several months).

From the paragraph above it paints a picture of a possibility of a reliability failure of the software (product) the company was using. Now the questions that should be asked: is this a software reliability issue; if so, whose fault is this; who does the company blame for the loss of revenue; how does the company fix itself going forward; how do we learn from this?

I was not privy to the advice provided on how the company should correct this incorrection; therefore, this is my opinion on considerations one would take to prevent this from happening (well hopefully).

One of my actions to correct the ship would be to make a requirement that all employees take a computer safety/update course on an annual basis. The insider that opened the attachment was clearly an employee that began this virus attack. Whether the employee did not fully understand the threats or there was some other motivation I cannot speak; however, implementing this requirement this would at least assist in keeping the employee's knowledge updated concerning cybersecurity.

Second thing would be to look at the day-to-day operations of the company's information technology team (IT). It is abundantly clear someone did not do their job effectively. The windows server software was not updated in a timely manner. Why IT did not do this is beyond comprehension; however, if they would have kept the software up to date then it would possible the vulnerability would have been caught. The back-up drives being in a failure state is another consideration; if they would have caught the back-up failures, they could have simply started the servers anew. And finally, the antivirus software was not updated which again questions what was IT doing all this time? Why were these infractions not

caught and for several months? Personally, I would have let the entire IT department go for gross negligence; but that is not my decision.

Third thing I noted and did not see in the write up was, did the company (this is Microsoft) promptly inform the consumer about critical or monthly software updates; and if so, was IT getting them? To me, this is a similar situation when the car company sends a recall notice for something detrimental that needs to be corrected. You get it fixed or risk fatal consequences. I know that Microsoft sends notices to their customers to let them know when updates are coming, what the updates are fixing, etc.

This is a long-winded blog, and apologize, I wrote this because I wanted to illustrate that sometimes the blame for reliability of products does not fall solely on individuals or entity; sometimes reliability is a team collaboration to keep this product running in tip top shape. If somebody within the group fails to do their due diligence, the entire team is culpable for the eventual failure of any product reliability.