**Final Debate**

**CS & SE 3162**

**Alex Lundin**

**Topic**

Security Protocols – should a small company be able to provide a subpar security system for customer database access that meets project objectives?

**For subpar security systems essay**

**Opinion**

I feel that allowing small companies to provide subpar security like this is an ethical decision.

Allowing a subpar security system increases total number of active projects. One fact to back this up is any time we regulate a business the result is some loss of total projects because the underperformers cannot meet the regulations. The Standish Group produces a report called the CHAOS report that analyses the main reasons for IT project failures. This report categorizes projects into three categories: success – the project was delivered on time, on budged and will all feature, challenged – the project was eventually delivered but either over budget, not on time or not fully completed and failure – nothing was delivered [1]. To support my statement that regulation causes loss in projects, the Standish Group reported 31.1% of projects in IT were outright cancelled in 2017 [2]. Tighter security enforcement will inevitably put more projects into this category

Allowing a subpar security system allocates more time for development of core features. The Standish Group reported 52.7% of software projects are completed behind schedule in 2017 [2]. I think extra requirements for security would leave less time for core features, extending schedule significantly.

Allowing a subpar security system saves businesses money because security systems are, for the most part, not revenue generating features. Security systems are preventative measure. Shareholders and end users might not pay for them, since the direct result in unapparent

**Trend**

It’s clear from the report data that I mentioned that stricter security protocols will cause these trends. We will see an Increase in project cancelation. We will also see an increase in project lateness. And finally, shareholders and end users will notice an increase in project cost. This will all trickle down to every day products since our entire society runs on software. We will see each of these three effects in everything from phone applications to grocery store prices.

**Impact**

There will be three positive impacts from allowing lower security measures. The first, is total developer jobs will increase. Second, products will be built faster with less regulation on security. And third, products and services will cost less to the consumer.

There is one major negative impact. Obviously, less secure software is riskier. My rebuttal to this is life is risky. Every time we step outside, we are incurring a risk. Telling everyone to stay inside to mitigate this risk is patronizing and so would enforcing security standards on small companies.

**Against subpar security systems essay**

**Opinion**

I feel that allowing small companies to provide subpar security like this is not an ethical decision for three reasons. Subpar security systems increase in quality between malicious tech savvy users. Today our user base ranges from non-tech savvy individually who can still manage to navigate the web all the way to senior architects who would the fantastic tools we use and love. This gap provides malicious tech savvy users plenty of opportunity to exploit unknowledgeable users and subpar security systems only perpetuate this. Subpar security systems are the wrong thing to build ethically. From a common-sense perspective, we would not allow a small elevator company to skip some safety measures just because they are a small company. In the same sense we should not allow a small software company to disregard security systems of projects they are building. Finally, subpar security systems allow snooping eyes into your home and personal space. This would enable “Big Brother” to survey the general population.

**Trend**

It’s clear from…

**Impact**

There will be three positive impacts from not allowing lower security measures. The first, is increased equality between the ranges of users. Second, software developers will be building the right thing ethically, so other professions will view us as a “full-fledged” engineering discipline since we adhere to a code of professional practice of doing the right thing. And third, we will have more privacy from snooping eyes.

There are two negative impacts. Obviously, more secure systems take longer to build, and they cost more to build. My rebuttal to this is, cheaply build products provide cheaply build benefits. We’ve all bought low quality products before an we know how disappointing this can be. Software is inheritably complex so we must pick our poison so to say. Nothing worthwhile comes without a cost, and this is true for security in software.

**References**

[1] https://getlevelten.com “CHAOS Report”. [online] Available at: https://getlevelten.com/wiki/chaos-report [Accessed 27 Feb. 2019].

[2] https://speedandfunction.com “A LOOK AT 25 YEARS OF SOFTWARE PROJECTS. WHAT CAN WE LEARN?”. [online] Available at: https://speedandfunction.com/look-25-years-software-projects-can-learn/ [Accessed 27 Feb. 2019].