Brandon Norton

CYSE 200T

April 22, 2025

Professor Duvall

Trust

BLUF: Trust is no longer just a social construct rooted in human relationships—it now extends to cybersecurity, as our increasing reliance on technology demands confidence in how our most private and sensitive information is protected.

Protecting the CIA Triad

 Trust in our information systems is fundamentally built upon the principles of the CIA triad: confidentiality, integrity, and availability. These principles aren’t just technical guidelines, they serve as a universal benchmark for assessing whether a system can be trusted to handle sensitive information properly or not. The three pillars define what it means for information systems to be secure. Confidentiality ensures that private information remains inaccessible to unauthorized personnel, integrity ensures that information remains whole and unaltered, and availability ensures that information remains readily available for those that require it and are given access. When any pillar of the CIA triad fails, it doesn’t just compromise data—it undermines the foundation of trust between companies and their users [1]. I personally believe that this trust aspect is harder to recover from than the technical anomalies. Misaligned firewall settings or computer viruses are relatively easy for an experienced technician to fix. However, repairing customer trust after an exploit, especially one that could have been prevented with better preparation, is significantly more difficult. We have seen this play out repeatedly across the world, affecting billions of users. Some individuals have even been subjected to multiple breaches by different companies and services. One of the largest examples in recent history is the Equifax data breach. Over 800 million users and 88 million businesses worldwide suffered a data breach where their names, addresses, birth dates, and Social Security Numbers were leaked (Breachsense, 2024). In the United States alone, over forty percent of the population (~145 million users) had their information leaked.

The Ramifications of Losing Trust

 When nearly half of the U.S. population has their most sensitive personal data exposed in a single breach, the question of “can we trust tech?” evolves from a small concern to a full-blown cultural conversation. When users no longer believe that their information is safe, they often withdraw, which damages business sustainability. Customers will delete accounts, cancel subscriptions, and stop using a product not as an act of defiance or betrayal, but as a precaution for their own safety. Loss of trust equates to a loss of reputation, which has a direct influence on a company’s revenue [2]. In 2013, Yahoo suffered a data breach that compromised all three billion user accounts, marking the largest data breach of all time. The data breach wasn’t the sole cause of the reputation hit, however. The breach occurred in August 2013, Yahoo didn’t notify its users until December 14, 2016, over three years after the incident. As customers were not aware of the breach, hundreds of millions of customers continued using compromised emails and passwords for years, subjecting themselves to further breaches, phishing attacks, identity theft, and fraud. The breach was so impactful and mismanaged that even the FBI and Congress had to step in and perform an investigation (StrongDM, 2025). The complete failure to address the data breach cost the company $117.5 million in a class-action settlement, $35 million in fees from the Securities and Exchange Commission, and another $80 million dollars in a settlement to the shareholders. The value of the company also dropped by $350 million before it was finally sold to Verizon in 2016, due to a lack of profitability and failing to innovate and adapt to a rapidly evolving internet landscape—I think the data breach had a direct impact on Yahoo’s collapse and eventual sale. I don’t believe that the users are to blame for being hesitant or even dismissive of our tech driven world—I blame the companies that prioritize innovation and profits over safety. I blame the CEOs and executive leaders that don’t see cybersecurity as an issue until a catastrophic data breach lands them in legal trouble with a hefty price tag. Finally, I blame governments for failing to hold companies accountable—and for ignoring the importance of securitization in shaping how companies are allowed to operate.

Steps Forward: A Change in Culture and Policy

 I don’t believe that the solution to restoring trust is a futuristic technology that doesn’t exist yet, or some piece of tech that is too expensive to implement—I believe it’s a cultural shift that companies and governments must agree upon. This means rethinking values, redefining the importance of cybersecurity, and reassessing where it fits within the larger picture of an organization’s mission. Cybersecurity is not an optional, niche subject; it must be embedded into the core of every company’s operation. All hands must be on deck when it comes to all facets of cybersecurity, which includes everyone from the employees to the executives. Cybersecurity isn’t only about being reactive to network incidents and breaches; it’s about being proactive in stopping them from happening in the first place. Training is paramount in securing a network and having a robust mandatory training program that go beyond checking the boxes is a step in the right direction. But training alone can only go so far—robust cybersecurity also requires significant investment in the right technologies to effectively secure a network. Companies cannot be held solely liable for this task alone, however; governments need to be consistently raising the bar. Adding new regulations like EU’s GDPR is a step in the right direction, but failing to enforce these regulations should be met with serious, real consequences. For instance, companies that delay breach disclosures or deceive the public about the breach’s impact need to face more than fines; they need to be held under a microscope and audited extensively until the issue is resolved and then receive additional audits to ensure that the policies are still being enforced. I have witnessed these scenarios play out repeatedly and it is frustrating to see record growth amongst these companies while also ignoring the security of their own customers. Without a cultural shift that prioritizes security, incidents like Yahoo and Equifax won’t be exceptions—they’ll be the norm. [3]

Conclusion:

 Through the lens of the CIA triad, we’ve seen how important confidentiality, integrity, and availability are in securing a system, and we’ve seen the aftermath when those pillars collapse. At its core, cybersecurity isn’t just about protecting information, it’s about protecting people. Every piece of information from emails to passwords, to Social Security Numbers, to addresses was provided to these companies for a reason: because the customers believed in the company to keep their information safe in exchange for better products and services. When that trust is shattered because a company failed to secure the information or notify the customer when they suffered a breach, the damage goes further than financial loss. This kind of failure cannot be solved with an apology or a lawsuit; it requires a shift in the company’s mission. This kind of change is not easy, nor is it cheap. As stated before, cybersecurity is no longer a small niche subject, it must serve the foundation of a company’s values and long-term mission. Only then can they maintain customer trust and loyalty. Without this, companies risk losing the very people who made them successful in the first place.

References

*Breachsense. (2024,* December 8). *Equifax Data Breach Case Study: Causes and aftermath. https://www.breachsense.com/blog/equifax-data-breach/*

StrongDM. (2025, March 18). *Yahoo Data Breach: What happened and how to prevent it*. https://www.strongdm.com/what-is/yahoo-data-breach#:~:text=The%20company%20paid%20a%20%24117.5,share%20price%20dropped%20in%202016.