What's the Deal with Security Vulnerabilities?

Why do we keep having breaches and security vulnerabilities? I think it comes to two main ideas. The first was talked about in lecture being the concept that cyber attacks are asymmetric in the attackers favor. They can take as much time as they want and use as much computing power as they need to brute force passwords or find vulnerabilities to steal credentials, which the Verizon DBIR says, "Over 80% of breaches within Hacking involve Brute force or the Use of lost or stolen credentials." On the flip side, the security team may have limited resources and time given to them, and as said in lecture cyber systems are very expensive. This could lead to being unable to fix every single potential security issue, so only major pressing issues get patched and leaving others vulnerable. That vulnerability can still be used in combination with others known and unknown to the team to breach the company.

Why do security vulnerabilities in software exist in the first place? Why do systems get misconfigured and left vulnerable? Why does phishing succeed? Well, these things happen because of the second and much more pressing cause of security issues, human error. Mistakes will happen, and no one is free from this. The Verizon DBIR says that phishing, misconfiguration, and misdelivery are 3 of the top 5 causes of breach, so it is clear that these mistakes can have a large impact. Now while the Verizon DBIR doesn't exactly mark phishing to be caused by human errors, I believe that the main culprit behind the existence of phishing stems from one's mistake or lack of understanding ultimately making it an error that one does. On top of this, we talked in lecture about the fact that cyber systems are complex and not understood well. This makes it far easier to make one tiny error in a program or configuration and, following the butterfly effect, creates an easy attack point that can be used to gain root privileges, access personal health data, or something equally as horrifying.

Why don't we catch them faster and how does this compare to other professions? Well as we talked about in lecture there is the idea of alert fatigue. An automated alert system may set off an alert but may be disregarded or deemed as a waste of time or burden, and now some team of attackers have gotten onto a system. This follows the butterfly effect and now they move on gathering info, gaining credentials, and accessing private information. This then finally gets caught and the emergency response is on them having to follow procedure and gather info on what the attackers have done first. Then, they fix how the system was breached in the first place. This is just one theoretical way an attacker could get on a system in a virtually infinite number of ways. Now, compared to other professions, IT / security is just about the only one where you don't see a threat to a workplace happening. These kinds of attacks are much harder to see and stop than a real life attack.

What are a few possible options that would eliminate security vulnerabilities forever? I personally don't think that much less than infinite time and money could really eliminate all potential vulnerabilities forever in software or any cyber system. However, even then, the human use of such a perfect system could still have errors occur or insider threats to break such security of the system. The other option would be to completely disconnect the system for the outside world making it essentially just a useless box. This is why no system could be 100% secure that is still usable, especially online. So how far could we go to getting rid of all vulnerabilities? Well to essentially remove software vulnerabilities, we need to constantly review and test the web software we use. We need constant monitoring of workers and servers to catch "evil" insiders and catch the technically impossible intruders. As well, we need to enforce secure practices for all workers and customers/ users with things like phishing, passwords, and multifactor authentication. Basically, the system needs to go into a semi-

lockdown mode where every action is watched internal and external and workers are ensured to only access what they need. Virtualization is everywhere, access control is perfect, and guards are everywhere. In the simplest of terms, this is what the US government does with its intelligence agencies but pushed to its max. However, even that is not infallible to insider threats and human error.

Basically, lets say my described system is “untouchable” but is still online. Such a system becomes very hard to use as is intended. In the corporate world, this system would probably cost insane amounts of money and may decrease productivity within the business especially within non-IT workers who aren’t used to high amounts of security like multifactor authentication on their systems and logins. As well, this “perfect” system becomes a near 1984 like system with constant monitoring. From “A Gift of Fire” textbook, it is mentioned that workers could file suit if they believe that the system invades their reasonable expectation of privacy in the workplace. So if workers aren’t well informed and clear terms aren’t set such a high level of monitoring could be considered a violation, and the company will have to handle the following lawsuits. As well, people may not want to work for such a business that has a high level of monitoring further hurting the business. On the term of ethics, this system as described may not have much of any ethical dilemmas as long as people consent to partake in such an intense system. However without their consent, it becomes a utilitarian ethical debate of whether the benefits of preventing all possible security risks outweighs the damages of having to monitor everything everyone does without their consent. Overall, the real life restrictions to perfect security are going to be people’s willingness to be monitored, which in the US people are not very willing, and the extreme financial and efficiency costs of creating a system.