The reasons for the 2018 Cybersecurity Policy are widely varied, from recognizing a need to prepare for the growing number of cyber attacks around the world, to needing to prepare for the 2020 Olympic Games, that were to be held in Tokyo. The influx of internationals would have opened the nation to cyber attacks from inside their own borders, so this was a huge concern. On top of that, Japan is very much a nation that is technologically stuck in the past. It's not all that uncommon to still see fax machines, older style computer desktops, and piles of loose paperwork throughout Japanese workplaces, including those critical to Japanese infrastructure. With the proposed 2018 policy, and a broader emphasis on Public-Private Partnership (PPP), they sought to address these issues (Watanabe, 2019).

Japanese society has a very uniform feel to it. Everyone must fit in, strictly following the rules and subtext of society, generally to avoid "rocking the boat"; those that don't tend to be at risk of being ostracized, or outcast. It's much the same in the Japanese workplace as well. Older technologies and policies are still in effect decades after they should have been replaced with more modern practices, but the societal uniformity isn't solely to blame. Japan has slowly aging workforce, many of whom have already or will soon reach retirement age, and many of whom hold managerial positions within enterprises. Having worked with this antiquated technology for decades with little issue, they see no need to adapt to the times; "if it isn't broken, don't fix it" would fit perfectly with this mindset. Japanese social uniformity, as well as an aging mindset has left them slow to adapt to technological changes like the Internet of Things (IoT) and opened them up to increased cyber attacks from outside forces (Hirasaka et al., 2021). The 2018 policy

sought to address this by improving cooperation between private and public enterprises to provide training, education, and mitigate risk posed by aging technologies.

One of the consequences was of course that these enterprises had to start taking steps to adapt to the times if they had not started already. This caused, and still causes interruptions in critical infrastructure, services, and IoT, as well as "growing pains" from enterprises needing to adapt to new technologies. This also led to an increased amount of data being shared by companies, and through data breaches both incidental, and via malicious intrusions. This in turn caused financial losses for enterprises thanks to their evolving security being compromised, which led to more disruptions (Japanese NISC, 2018). In the short term, these damages were significant, but in the long-term, these were simply the side effect of decades of workplace stagnation, followed by a rapid need to evolve to current times, and security concerns.

These concerns are part of what prompted the inclusion of the PPP initiative, and a focus on educating the Japanese public about cybersecurity in the 2018 policy. It also outlined, especially for companies, the need to view cybersecurity measures as company investments, rather than optional security measures. While the public may be wise to the benefits of cybersecurity, many business leaders in Japan at the time still viewed them as wastes of resources, and an extra cost for something that wasn't even guaranteed to occur to them. This led to the policy outlining a supply chain of cybersecurity devices, as well as guidelines and plans for smaller enterprises, without the ability to develop a sophisticated cybersecurity apparatus (Japanese NISC, 2018). All of this in addition to the PPP, was developed around the idea of developing critical infrastructure to protect Japanese society from the risks of cyber-attacks. One attack could cascade into a disaster for Japanese society but helping their aging enterprises to adapt to modern technologies would lessen long-term risks to their government and their people.

Works Cited:

Hirasaka, M., Kusaka, Y., & Brogan, J. (2021). Japanese style management in eras of change: new management model. *SN business & economics*, *1*(6), 85. https://doi.org/10.1007/s43546-021-00087-0

Japanese National center of Incident readiness, and Strategy for Cybersecurity (NISC). (2018, July 27). *Cybersecurity strategy - 内閣サイバーセキュリティ...* Retrieved April 11, 2023, from https://www.nisc.go.jp/eng/pdf/cs-senryaku2018-en.pdf

Watanabe, K. (2019). PPP (Public-Private Partnership)-Based Cyber Resilience Enhancement Efforts for National Critical Infrastructures Protection in Japan. In: Luiijf, E., Žutautaitė, I., Hämmerli, B. (eds) Critical Information Infrastructures Security. CRITIS 2018. Lecture Notes in Computer Science(), vol 11260. Springer, Cham. https://doi.org/10.1007/978-3-030-05849-4_13