Introduction

The 2018 Japanese Cybersecurity Policy outlines Japan's increased reliance on modern Internet of Things (IoT) technology, it's incorporation into critical infrastructure, the risks associated with them, and the possible losses expected by "state-sponsored incidents". It explains and expands on how different devices such as phones, appliances, and vehicles contribute to a united Cyberspace front, as well as the risks it poses to everyday citizens, and the country. The strategy goes on to outline basic objectives, assurances, and goals through 2021. It also takes into account incident readiness and recovery, a problem which increased worldwide throughout the implementation of this strategy. Finally, one of the most important things this strategy does is it promotes cooperation between government bodies, industries, educational institutions, and the citizens of Japan to help improve awareness foundational cybersecurity knowledge throughout the country (2018 Cybersecurity Policy of Japan, 2018).

The policy was developed to address Japan's rising reliance on IoT technologies throughout the country, addressing its positive impact, and potential risks facing it. It begins by defining what "real space" and "cyberspace" is, devices related to it, and how it all comes together to form a united front, composed of many aspects from cyber space, and real space. This united front has led to advancements and innovations throughout both industry and society, as well as revolutionary new tech including virtual reality, AI, and the wide availability of information (2018 Cybersecurity Policy of Japan, 2018).

It also addresses the threats facing these new technologies, and their reliance on it which can quickly be out of their control, and lead to losses throughout their society, industry, and economy. This has led to an increased focus on risk assessment, incident recovery, and

interdisciplinary cooperation. This emphasis on cooperation throughout different sectors of the country seeks to build a foundational knowledge of cybersecurity, and the risks associated with IoT tech throughout its society, potentially lessening risks, and raising awareness and education regarding cybersecurity that has been lacking in years past (Neuran et al., 2016).

Two of the biggest reasons for this new policy being international in nature; those reasons being the (at the time) upcoming 2020 Tokyo Olympics, and the rise in state-sponsored cybersecurity attacks. With the influx of so many international citizens, and the massive boost in tourism the country would have had from the Olympic events, a lacking cybersecurity policy would have meant potential damage to national infrastructure, and tourists, but to the economy as a whole (2018 Cybersecurity Policy of Japan, 2018).

Another reason was the rise in cybercrimes, which around this time were both growing in scope, effect, and had hints of state-sponsorship behind them. During the winters of 2015 and 2016, Ukraine was subjected to cyber-attacks on their electric infrastructure which led many to believe (at this point, rightfully so) that Russia has prompted the cyber attack to test their capabilities (Mori & Goto, 2018). A cyberattack on a city like Tokyo could heavily damage their economy, cripple their nation for a time, and hurt their standing as a nation. Measures had to be taken to negate this possibility.

These were 2 of the biggest reasons that led Japan to start reconsidering their cybersecurity capabilities and reassess their national policies. The growing international threats, and lacking cyber defenses led to a steady revamp of not only their recovery procedures, but a nationwide emphasis on education on the subject. An population educated on cybersecurity matters, coupled with an enhanced risk assessment procedure, and recovery plan was just what Japan needed to begin re-vamping their security.

Works Cited:

Government of Japan. (2018, July). *2018 Cybersecurity Policy - JAPAN*. www.nisc.go.jp. Retrieved February 5, 2023, from https://www.nisc.go.jp/eng/pdf/cs-strategy2018-en-booklet.pdf

Mori, S., & Goto, A. (2018, July 11). *Reviewing National Cybersecurity Strategies*. www.jstage.jst.go.jp. Retrieved February 8, 2023, from https://www.jstage.jst.go.jp/article/jdr/13/5/13_957/_pdf/-char/ja

Neuran, R., Chinen, K.-ichi, Ten, Y., & Shinoda, Y. (2016, October 14). *Towards Effective Cybersecurity Education and Training*. dspace.jaist.ac.jp. Retrieved February 5, 2023, from https://dspace.jaist.ac.jp/dspace/bitstream/10119/13769/1/IS-RR-2016-003.pdf