Summary Post to Discussion 1

The developed world has grown critically reliant on a connected, software backed, global network. Michael (Oseji, 2021) adds that with the advent of IoT devices in both homes and businesses, exposure to a broader range of risks is inevitable. This increasingly complex network is the backbone of everything from industrial processes to the R&D of lifesaving drugs (He, Frost and Pinsker, 2019). This has also led to increasing odds of being compromised and an increasing draw to do the compromising. We have shown that the cost of attacks can extend far beyond purely monetary loss. Examples such as the Merck & Co (He, Frost and Pinsker, 2019) or Maersk (Wilson, 2020) cyber-breaches provide insight into the importance of the adage, “an ounce of prevention is worth a pound of cure.” Both these companies faced significant monetary setbacks as well as significant externalities, realized a tarnished reputation, setbacks to R&D, crippled supply chains and lost productivity throughout the general operations.
Jan (Küfner, 2021) points out that despite an increasing need for sound cyber policy in business, the requirement is often overshadowed at the product delivery level by tight deadlines and a pressure to bring goods to market without considering the more secure, but time-consuming route of incorporating secure development or cybersecurity into the design phase. This being especially true of startup businesses eager to break the barriers of entry to a market.
Regardless of a business’ tolerance for risk, in the long run there is very little to be gained by figuratively rolling the dice on cybersecurity. Faster delivery of a good or service may increase growth and market share, but it also increases the target surface area. Charlotte (Wilson, 2021) succinctly points out that security is not a function of a single department or person, but as a company. In today’s landscape it is the role of everyone to be aware of cyberthreats and to have an adequate understanding in identification and avoidance of said risks to avoid the potentially devastating impacts of a cyber-breach.

References:
He, C.Z., Frost, T. and Pinsker, R.E. (2019). The Impact of Reported Cybersecurity Breaches on Firm Innovation. Journal of Information Systems, 34(2), pp.187–209. Available at: http://content.ebscohost.com/ContentServer.asp?EbscoContent=dGJyMNLr40SeqLQ4yNfsOLCmsEmep7dSs6m4Ta6WxWXS&ContentCustomer=dGJyMPGvtkmyqLdNuePfgeyx9Yvf5ucA&T=P&P=AN&S=R&D=bsu&K=145694392 [Accessed 11 Feb. 2021].

Küfner, J. (2021) Discussion Forum post by Simon Miller, 31 January

Oseji, M. (2021) Discussion Forum post by Simon Miller, 8 February

Wilson, C. (2021) Discussion Forum post by Simon Miller, 9 February