BENS Technology & Innovation Council – Recommendations for the Secure Introduction of 5G to Business Operations

5G – the latest iteration of the mobile telecommunications network – is predicted to revolutionize business operations and, significantly, stands to strengthen the network's security structures. Nonetheless, 5G is not infallible. Its ability to share information through a web of connected devices, at lightning-fast speed and ultra-high reliability, introduces increased levels of complexity and relative novelty through which new and unique security challenges have been born. Adoption of 5G must therefore include a proper assessment of the risks involved and plans for protection, vigilance, and remediation of these new security challenges. In light of this, the BENS Technology & Innovation Council recommends the following actions:

1. **Create a Cross Functional Team**, representative of the whole enterprise, to:
    a. **Define the Use Case** as a basis for further integration planning.
    b. **Evaluate Availability of Applicable Talent** in the business, and determine whether current staff require augmentation or additional training.
    c. **Build off 4G Security Protocols** to determine which existing security protocols can be retained.
    d. **Determine an Optimum Adoption Timetable** with consideration to the benefits of being an early vs. late adopter.
2. **Ensure Leadership Buy-In**, ensuring everyone is aware of the risk-benefit analysis and the most appropriate timeline for the business to integrate 5G into operations.
3. **Develop a Threat Identification Plan**, encompassing both hardware and software as it is introduced into business operations.
4. **Create an Employee 5G Use Policy**, plainly stating which 5G elements can be introduced into the enterprise, the process for procuring and introducing those elements, and exceptions to the policy.
    a. **Develop a Connected Devices Integration Plan**, mandating security controls and standards on 5G devices connecting to the network.
5. **Develop a Patch Management Plan** to ensure known software and hardware vulnerabilities are continually fixed.
6. **Understand the Limitations of Service Providers and Third Parties** through an assessment of which assets are in their networks, what network hygiene practices are being employed, and whether the network slices are appropriately isolated.
7. **Employ Thorough Hardware Vetting and Standards Enforcement** by regularly re-assessing use-case standards, hardware supplier trustworthiness, and security configurations.

Through the adoption of these practices, businesses can maximally mitigate the often under-reported risks associated with 5G. Private enterprise can lead the way in developing a security-minded culture across the whole nation by itself adopting the right focus on security, as 5G is introduced into the economy.

For further details, please visit the BENS 5G – A Guide to Secure Adoption by Business webpage.