A Resolution for Corporate Network

To handle the hackers around the world. Please use Desktop or Laptop without WIFI Function use "ETHERNET CARD" to connect all the PCs together. Let say for instance Bank Industry. Each teller or counter's PC is connected with "RJ45" cables to the "ETHERNET CARD". I assume and suppose the PCs of teller and counter cannot connect outside INTERNET world. They cannot browse Website and access the "World Wide Web". As I said, close area network is the UTIMATE solution. You create your own small BANK area network, without accessing outside. Programs development, emails, documents, storages.... can be only access by your enterprise. You can still use ROUTERS and SWITHCES and all those routing methods, the main point is don't access or allow to be access from the outside world!! You may argue you need to access overseas countries! Yes, as I said minimize the chance of being Hack. As I said Hong Kong has an underground copper sea cable that is built under the sea across the "Atlantic Ocean", that is link to "England". You can perhaps make an agreement with now call "Hong Kong Telecom", to lease a line. That means You have a large close area network that span across 2 countries.

This kind of close area network advantages are: You are focusing on your JOB, without disturb by outside internet world. I assume you will not be watching TIKTOK during programming development. You will not need to download malware or unlicensed software. But programs need packages or software... in order for development. Ah... I think enterprise has their own software repository (licensed software, authorized freeware...), that have its own communities for approving and being security checked. This causes enterprise employees without violating copywrite rules. But employees need to access outside world to look for information. Right so they can bring their own laptop or perhaps provide one allow them access outside internet. But these laptops or PCs are strictly not allowed to connect to the enterprise internal network. Rules maybe they are not allowed to have "ETHERNET CARD" installed on their laptop or PCs, they are only allowed to use WIFI. This way they can never connect to the corporate system and can achieve information and knowledge around the world. USB or other external devices are not allowed to use. So, the corporate does not have USB, DISC driver installed on their PCs. How about Home working? as minimized the chance of being hacked. The only way is you can only use the corporate provided PCs or Laptops. This kind provided Laptops or PCS has installed Enterprise Grade Security Software and Complicated connection method to connect to the corporate internal system. Another advantage has less malware or viruses, because you are not accessing outside, internal emails are being internal scan, so as to decrease the chance of being malware affected. Also lower the costs of installing large complicated anti-virus systems to monitor your corporate laptops and PCs. The only disadvantages are you should have a naming standard or IP numbering standard of each laptop and PCs for the corporate. But this should not be a really a problem. Several large network can be grouped as a small sub-network. As you are creating your own internal network, you are not consuming the outside world IP addresses which is nearly being filled up.

That is why they are suggesting using IPV6 in replacing IPV4.