The IoT 2020 Pledge

Not knowing what is or is not attached to a corporate network – including the security status of each device – is an irresponsible position for any organization to take. That is why we are urging organizations globally to take what we call the IoT 2020 pledge.

By the end of 2020, organizations will pledge to:

- Write and implement rules restricting IoT devices that can be attached to any organizational network to those that are approved by our information security specialists. This includes devices procured by the company as well as those supplied by employees, contractors, vendors or others.
- Inquire into the security status of each device for which a connection request is received. Only those devices with reasonable security will be approved for connection to company networks. However, other devices may be approved for connection to a guest network that is totally separate from and not connected to company networks.
- Implement controls to enable the real-time inventory, monitoring and control of devices connected to company networks so we may know when a new device is connected. This will give us the option to reject connections of devices that have not been preapproved by the information security unit.
- Provide information to our employees on these safeguards and require compliance.
- Inquire into the IoT policies of any business partner, supply chain partner, vendor or other external organization that is authorized to connect to our network to determine if their devices represent a risk to our networks and will take appropriate steps to protect our network security.
- Work with our internal auditors, corporate/agency compliance specialists and external security review personnel to assure that IoT is included in reviews, audits and compliance work to help ensure that our policies are implemented as intended.
- Update our IoT-related policies regularly to keep up with changes in technology.
- Include the status of our IoT-related security plans and operations in our reports to senior management and the board of directors.
- Revoke access to IoT devices and software with known (or discovered) vulnerabilities and poor security design without greatly impeding business efficiencies.