How IoT is Changing the World

Posted by Ronald van Loon on February 23, 2017 at 7:30am View Blog

Digital Twin:
Digital twin refers to a digital replica of physical assets, processes and systems that can be used for various purposes. This pairing of the virtual and physical worlds allows analysis of data and monitoring of systems to head off problems before they even occur, prevent downtime, develop new opportunities and even plan for the future by using simulations.

Cognitive Commerce:
Use of a spectrum of technologies, ranging from speech recognition to a recommendations system based on machine learning. Use an in-depth understanding of customers' behaviors and preferences, both at aggregate and individual level.

Predictive Maintenance
Using IoT issuing an alert before a machine or equipment breaks down.

Connected Devices
Allowing users to control their smart devices from a remote location.

Who Will Rob You on the Digital Highway?

By Ton Slewe and Mark Hoogenboom

- Security terms
  - Confidentiality: privacy, authorization, exclusivity;
  - Integrity: correctness, completeness, validity, authenticity, auditability, non-repudiation;
  - Availability: continuity, timeliness, contingency, reliability, robustness.

- Emerging Trends in Security Threats
  - A shift from generic attacks to more sophisticated and well targeted attacks
    - Tips: using a separate hardware token; detection of attach
  - Increasing propagation speed and volume of virus attacks—these viruses may contain Trojan horses;
  - Increasing speed of the release new of viruses and attacks after the detection of a vulnerability;
    - Tips for both 2&3 : In addition to the efforts to prevent or invalidate such attacks, financial organizations should also have intrusion-detection systems in place and have computer emergency and response teams to repress attacks
  - Increase in identity fraud.
    - Tips: better method of detection of identity fraud
- Overall: having a good monitoring and detection system in place, responding quickly to new security threats, and adapting appropriate security measures as required. Golden rule: reaction time to attacks should not exceed the time it takes an attacker