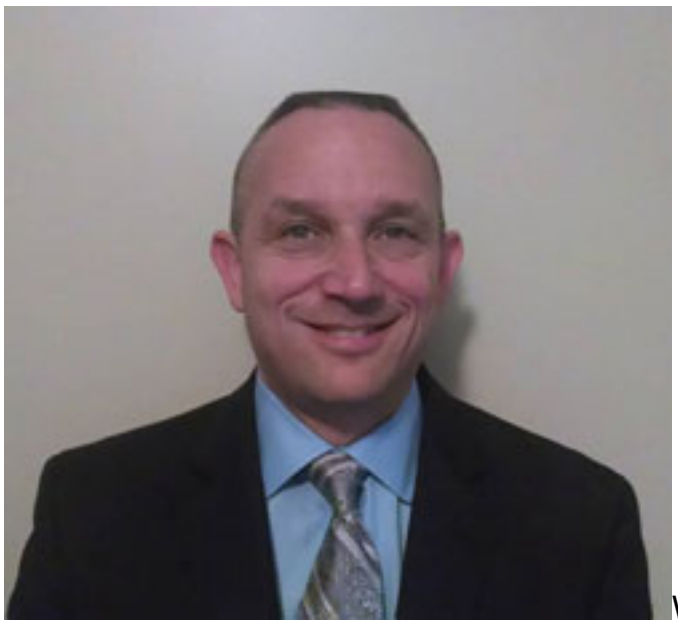
M2M + Security + Cloud = Love

Marie McGehee, Director of Corporate Communications, Verizon Enterprise Solutions

 With sensors and networking technology being strapped to nearly every machine around the globe at a blistering pace, estimates projecting 50 billion connected devices by 2020 may be too conservative.

Consider this scenario. Cities and municipalities want to control and monitor street lights remotely to save time, money and manpower. By monitoring the health and condition of street lights remotely, city workers aren't left with the task of checking each light, block by block, in order to identify a maintenance problem.

"By giving virtually every type of device the ability to communicate wirelessly, from ATMs and smart meters to street lights and connected cars, the Internet of Things (IoT) is at the vanguard of creating new business drivers for the manufacturing industry," said Jeff Feldman, Associate Director Global Enterprise Data Solutions at Verizon. "When we talk about the key benefits of deploying solutions such as logistics automation, remote monitoring and condition-based maintenance on connected machine-to-machine (m2m) technology, increasing operational efficiency is just the tip of the iceberg. It's also about improving decision making and accelerating response times which allows manufacturers across several industries to create new revenue streams and reach new customers in new markets and in new ways."

Feldman says that increasingly as manufacturers realize the benefits of wireless connectivity in order to improve communication with their devices to gain more robust data and analytics, that even greater emphasis will be placed on security and the cloud.

"Simply focusing on m2m in a vacuum as the wireless connection point for devices

is no longer considered a best practice today, Feldman added. "As connected solutions continue to play a pivotal role in transforming our lives [whether it's the way we receive healthcare, interact with our financial institutions, maintain our homes, or travel from point A to point B in the car and in the air] it's imperative that manufacturers take an integrated approach by also including security and cloud as a necessary part of the equation to mitigate risk and realize new possibilities."

Security, Security, Security

According to Verizon's 2013 Data Breach Investigations Report [1] (DBIR), twenty percent of network intrusions were targeted at the manufacturing industry. The report also noted that manufacturers were often subject to targeted social attacks exploiting human weakness in order to gain access to multi-functional malware or internal systems.

With hacktivism and denial of service attacks (DDos) continuing to make news headlines, Feldman says that private networks are being adopted more than ever by manufacturing clients as a key tool for protecting their assets.

"The stringent intellectual property requirements that exist in the manufacturing industry are even more crucial when that intellectual property is being moved around the world from machine-to-machine wirelessly. As a result of those requirements, we are private networking our manufacturing clients at a high percentage, which is a dedicated connection from Verizon to the customer's data center that never traverses the public Internet. Private networks have helped to alleviate some of the angst with security that comes with connected solutions. Clients can also add encryption for another layer of security," Feldman continued.

Although Verizon cautions against a one-size fits all security posture which may result in some organizations under-protected from targeted attacks while others potentially over spend on defending against simpler opportunistic attacks.

Taking a deeper dive into the IT security threats facing selected industries including manufacturing, and how to prevent them, this month Verizon unveiled its Industry Threat Landscape Reports [2] drawing upon three years' worth of data from the DBIR.

Interesting findings from the manufacturing study [3] include:

- While outsiders were the biggest threat, business policies and practices must take into account that the enemy often lies within
- 79 percent of IP thefts were only detected by external parties – such as law enforcement, fraud detection or even customers
- 62 percent of attacks took months – or even years – to detect.

Clouds on the Horizon

Feldman notes that as the volume of data and analytics available to manufacturers

increases in today's connected world, cloud computing will play a bigger role.

"The proprietary nature of the manufacturing industry has had a bit of a 'cause and effect' in the sector's exploration of cloud adoption in that they have been quite cautious historically. Many manufacturers have opted to stick with their own data centers maintained in-house. However, as the volume of data that they have in their arsenal increases exponentially, the benefits of migrating that data to an expandable and elastic enterprise-grade cloud has more appeal due to the economies of scale," said Feldman.

In its State of the Enterprise Cloud Report [4], Verizon draws upon data between January 2012 and June 2013 and examines current cloud adoption and usage trends—both in terms of how organizations are deploying cloud technologies and what they want from enterprise-grade cloud services.

Highlights from the report include:

- In the past year, enterprises increased their overall cloud spend by 20 percent
- Also, the use of cloud-based storage has increased by 90 percent. Verizon believes that this has been largely driven by the shift of business-critical applications to the cloud.

Parting Thoughts

Overall, in Feldman's view, the advent of m2m connections to foster wireless communication between "things" coupled with an enterprise-grade cloud environment to handle massive amounts of data in a secure way is not only optimal for manufacturers.... it's love!

For more information on Verizon's connected solutions for the manufacturing industry, visit
http://www.verizonenterprise.com/us/industry/manufacturing/ [5]

Links:
[1] http://www.verizonenterprise.com/DBIR/2013/
[2] http://www.verizonenterprise.com/DBIR/2013/industries/
[3] http://www.verizonenterprise.com/resources/factsheets/fs_dbir-industries-manufacturing-services-technology-threat-landscape_en_xg.pdf
[4] http://www.verizonenterprise.com/news/2013/08/2013-state-enterprise-cloud-report/
[5] http://www.verizonenterprise.com/industry/manufacturing/