50 Predictions for the Internet of Things in 2016

Posted by David Oro on December 29, 2015 at 4:05pm

Earlier this year I wrote a piece asking "Do you believe the hype?" It called out an unlikely source of hype: the McKinsey Global Institute. The predictions for IoT in the years to come are massive. Gartner believes IoT is a central tenet of top strategic technology trends in 2016. Major technology players are also taking Big Swings. Louis Columbus, writing for Forbes, gathered all the 2015 market forecasts and estimates here.

So what better way to end the year and look into the future than by asking the industry for their predictions for the IoT in 2016. We asked for predictions aimed at the industrial side of the IoT. What new technologies will appear? Which companies will succeed or fail? What platforms will take off? What security challenges will the industry face? Will enterprises finally realize the benefits of IoT? We heard from dozens of startups, big players and industry soothsayers. In no particular order, here are the Internet of Things Predictions for 2016.

Photo Credit: Sean Creamer via Flickr

Nathaniel Borenstein, inventor of the MIME email protocol and chief scientist Mimecast

"The maturation of the IoT will cause entirely new business models to emerge, just as the Internet did. We will see people turning to connected devices to sell things, including items that are currently "too small" to sell, thus creating a renewed interest in micropayments and alternate currencies. Street performers, for example, might find they are more successful if a passerby had the convenience of waving a key fob at their "donate here" sign. The IoT will complicate all aspects of security and privacy, causing even more organizations to outsource those functions to professional providers of security and privacy services."

Adam Wray, CEO, Basho

"The deluge of Internet of Things data represents an opportunity, but also a burden for organizations that must find ways to generate actionable information from (mostly) unstructured data. Organizations will be seeking database solutions that are optimized for the different types of IoT data and multi-model approaches that make managing the mix of data types less operationally complex."

Geoff Zawolkow, CEO, Lab Sensor Solutions

"Sensors are changing the face of medicine. Mobile sensors are used to automatically diagnosis disease and suggest treatment, bringing us closer to having a Star Trek type Tricorder. Also mobile sensors will ensure the quality of our drugs, diagnostic samples and other biologically sensitive materials through remote monitoring, tracking and condition correction."

Zach Supalla, CEO, Particle

"2016 isn't the Year of IoT (yet)- It's A Bump in the Road. The industry has been claiming it's the year of IoT for the last five years - let's stop calling it the year of the IoT and let's start to call it the year of experimentation. 2016 will be the year that we recognize the need for investment, but we're still deeply in the experimental phase. 2016 will be the bump in the road year - but at the end of it, we'll have a much better idea of how experiments should be run, and how organizations can "play nicely" within their own walls to make IoT a reality for the business."

Borys Pratsiuk, Ph.D, Head of R&D Engineering, Ciklum

"The IoT in medicine in 2016 will be reflected in deeper consumption of the biomedical features for non-invasive human body diagnostics. Key medical IoT words for next year are the following: image processing, ultrasound, blood analysis, gesture detection, integration with smart devices. Bluetooth and WiFi will be the most used protocols in the integration with mobile."

Brian T. Patterson, President, EMerge Alliance US Representative, International Electrotechnical Council

"IoT to Enable an Enernet 2016 will see the IoT starting to play a major role in the evolution of a new, more resilient, efficient, flexible and sustainable 21st Century electric energy platform. IoT connected sensors and microcontrollers will enable the effective and efficient management of a true mesh network of building and community level microgrids, which in turn will enable the greater use of distributed renewable energy sources like solar, wind, bio fuel micro-turbines and fuel cells. The convergence of data networks and physical energy grids will give rise to what will become the Enernet, a data driven transactional energy network."

Chris Rommel, Executive VP, IoT & Embedded Technology, VDC Research

"PaaS Solution Evolution to Cannibalize IoT Platform Opportunity: The landscape of Platform-as-a-Service (PaaS) solutions is changing rapidly. In 2015, leading PaaS providers IBM, Oracle, and SAP threw their hats into the "IoT platform" ring. As quickly as the value of PaaS solutions had been placed on the consumerization and user experiences of development platform offerings, premiums have now been placed on the ease of back-end integrations. However, the value associated with time to market in the Internet of Things marketplace is too high. IoT solution development and engineering organizations still want the flexible benefits offered by PaaS development, but they also require a breadth of out-of-the-box integrations to mitigate the downstream engineering and deployment hassles caused by heterogeneous IoT systems and networks topologies. The desire and need for enterprise organizations to tightly integrate deployed systems' operations with enterprise business functions are reshaping PaaS selection. The need for tight, out-of-the-box integrations extends beyond the back-end, however. Bi-directional integration is critical. The heterogeneous nature of the IoT and wide range of device form factors, components and functions is too complex and costly to rely on bespoke integrations. As such, we expect the aforementioned PaaS leaders to accelerate their ecosystem development efforts in 2016. Although we likely won't see any real winners yet emerge in the IoT PaaS space, I do expect that the investments made by the aforementioned large players to threaten the market opportunity available to smaller IoT-focused platform vendors like Arrayent and Carriots."

Laurent Philonenko, CTO, Avaya

"Surge in connected devices will flood the network – the increasing volume of data and need for bandwidth for a growing number of IoT connected devices such as healthcare devices, security systems and appliances will drive traditional networks to the breaking point. Mesh topologies and Fabric-based technologies will quickly become adopted as cost-effective solutions that can accommodate the need for constant changes in network traffic."

Lila Kee, Chief Product Officer and Vice President, Business Development, GlobalSign

"Prediction: PKI becomes ubiquitous security technology within the Internet of Things (IoT) market. It's hard to think of a consumer device that isn't connected to the Internet these days - from our baby monitors to our refrigerators to our fitness devices. With the increase of connected devices of course comes risk of exposing privacy and consumer data. But, what happens when industrial devices and critical infrastructure connect to the Internet and get hacked? The results can be catastrophic. Security and safety are real concerns for the Internet of Things (IoT) and especially in the Industrial Internet of Things (IIoT). Regarding security, the industrial world has been a bit of a laggard, but now equipment manufacturers are looking to build security in right at the design and development stages. Unless the security challenges of IIoT can be managed, the exciting progress that has been made in this area of connected devices will slow down dramatically. PKI has been identified as a key security technology in the IIoT space by the analyst community and organizations supporting the IIoT security standards. In 2016, we expect that PKI will become ubiquitous security technology within the IoT market. There will be an increased interest in PKI, how it plays in the IoT market and how it needs to advance and scale to meet the demands of billions of devices managed in the field."

Craig Macy, CEO and founder, Onstream

"As the world of connected devices and IoT emerges, the potential for true autonomous operation appears. Even now, the focus is almost exclusively on basic stimulus/response triggering, and simple "if this than that" automation. With 50 billion devices and a trillion sensors coming on line, simple practicality would suggest autonomy is a necessity. I strongly believe in 2016 we'll see the emergence of the Age of Autonomy – we'll build devices that are rationally adaptive, and have the ability to act based off of their environment, other devices, and self-awareness of their own condition."

Sagar Jethani, Head of Content, element14

"When it comes to the IoT, 2015 was the year of semiconductor consolidation. We saw major manufacturers like NXP and Freescale, Avago and Broadcom, and Intel and Altera come together. This trend is only going to continue as we get into 2016. What's driving this merger frenzy is the need for these companies to ramp up their response to more demands for IoT solutions, especially within the automotive industry. Today, a high end automobile can have over one hundred million lines of code. A Boeing 787, by contrast, has less than seven million. So these cars are really better thought of as rolling computers and engineers are increasingly pressed to design cutting-edge applications for owners and drivers. In turn, engineers are expecting solution providers to adapt to their needs. The companies that are going to do well in this new, hypercompetitive environment are those that can provide engineers with the assistance they need to come up with a good IoT framework of design across industries and applications."

Tim Tuttle, CEO and founder, MindMeld

"Voice UI device proliferation will require an ecosystem approach – such as a smart connected home ecosystem, as opposed to individual appliances having their own voice UIs. As we get to such a myriad of devices and applications, users will want to get a seamless experience and successful solutions will take an ecosystem approach. For example, in your home, you should not have to call the HVAC system separate from the security or lighting system. Rather the home ecosystem should know what you're trying to do and direct naturally spoken commands to the right service within the ecosystem."

Steve Schmidt, VP of Corporate Development, Flexera Software

"Intelligent Device Makers Will Look More Like Software Companies to Garner IoT Profits: Increasingly, the value of physical devices is defined by the embedded software inside of those devices, or the control software that helps to manage those physical goods. Simply selling more device units will not result in the massive spike in profits manufacturers are hoping for as they make a play to compete in the Internet of Things. Manufacturers will have to start thinking and acting more like software companies, leveraging the software applications they build into their products as a driver to reduce manufacturing costs, increase product innovation, and capture new revenue streams. Taking a software-centric approach means manufacturers will start re-designing products from fixed-function, disconnected devices to flexible, seamlessly connected systems. A software-centric approach will streamline all aspects of the supply chain, from manufacturing to monetization."

Lasse Andresen, CTO, ForgeRock

"Chip to cloud (or device to cloud) security protection will be the new normal As business technology advances, the security data chain continues to grow, presenting an increasing number of opportunities for hackers to break in. With most data chains now spanning the full spectrum of chip, device, network and cloud (plus all stages in between), many organizations are starting to realize a piecemeal approach to protection simply isn't effective. This realization is spurring the adoption of more 'chip to cloud' security strategies, starting at the silicon level and running right through to cloud security. In this model, all objects with online capabilities are secured the moment they come online, meaning their identity is authenticated immediately. In doing so, it eliminates any window hackers have to hijack the identity of unsecured objects, thus compromising the entire data chain via a single entry point."

Felicite Moorman, Esq., CEO, BuLogics and StratIS

"2016 will see rapid adoption of IoT platforms and subsequent return on investment in the commercial residential space (apartments and student housing), similar to technologies being promulgated in hospitality, including widespread use of electronic access and collaborative manager/resident environmental controls, like thermostats - all controlled via apps. The decrease in price of both hardware and software combined with an increase in rate of return, options, and demand will create unprecedented technology adoption and trajectory in this previously neglected market."

Photo credit: David Oro

Thorsten Held, Co-Founder and Managing Partner, whiteCryption Corp.

"Ransomware, a means whereby a hacker takes over a device and demands a ransom to remove the restrictions, will creep into biomedical devices in 2016. To thwart life-threatening consequences, medical device manufacturers will be looking for diverse ways to address these types of security flaws using more stringent, agile security solutions against the malware threats."

Mark Gazit, CEO, ThetaRay

"As the Internet of Things continues its growth and more and more machines become connected, we will likely see an increase in cyber attacks from hacktivists, terrorist groups and governments. Now that sophisticated hackers are gaining access to cars, airplanes, medical devices and more, cyberthreats that most people would consider science fiction are increasingly becoming reality."

JD Doyle, Chief Technology Officer, LinkeDrive, Inc.

"In the coming years, I believe that IoT will impact the Transportation/Logistics markets in the following ways: 1) We will see an increase in the utilization of environmental sensor data (traffic, weather, construction) and the ability to synthesize it in real time to improve navigation and delivery performance. 2) With wireless access to vehicles internal computers, there will be an increased need for maintaining privacy. Ensuring the security of vehicle control will be key challenges in the market. 3) The vehicle will step out as a key data collection platform for all types of business, environmental and social analytics."

Ashish Thusoo, CEO and Co-founder, Qubole

"IoT and the cloud. With the ever increasing amount of data produced through connected environments and apps, the need for big data and analytics is just getting more and more pronounced. As this market transitions to the mainstream, there is a need to simplify the process of unlocking big data insights. Cloud-based big data services are driving a lot of this, and increasingly making big data accessible in a simplified manner to the mainstream market. This trend will keep accelerating. We will also see an increased focus on vertical analytical applications in industries, such as the healthcare sector, that will further simplify the usage of big data and its overall adoption."

Clint Oram, Co-Founder and CTO, SugarCRM

"CRM and IoT will become intertwined: Smart companies want to stay a step ahead of their customers so they can provide information before the customer even knows they need it. Smart devices can offer new ways to deliver on that promise. The potential of harnessing the data of billions of connected devices and integrating that data within the CRM to create extraordinary customer relationships is very exciting. CRM platforms will evolve to work with the data that is being generated, making sense of that data and communicating to the people who can benefit from the analysis so they can perform real actions to help the customer."

Ed Abbo, President and CTO, C3 Energy

"In 2016, IoT and the digitized power grid will compel the traditional utility business model to evolve in meaningful ways, including energy theft. A whopping $6 billion of electricity is pirated in the U.S. each year, making it the third largest form of theft after shoplifting and copper theft. Just as credit card companies use historical spending data to flag potential fraud, utilities are starting to use big data and predictive analytics to identify sources of energy fraud, such as electricity being used in a household that has been vacated or is without a contract. In 2016, as utilities increasingly track energy consumption – including on inactive meters – they will also begin to predict and prevent fraud and recoup millions of dollars per year."

Mark Coderre, National Practice Director, OpenSky

"Attacks on connected cars, connected medical devices, and connected critical infrastructure have all hit the headlines in the recent past; and this is just the tip of the iceberg. The Internet of Things is proving to be a treasure trove for hackers. When developing networked devices, manufacturers are still placing more value on features than on security. "Security by design" must become an integral factor in development so that innovations win over increasingly security-conscious users. Additionally, the relevance of Cyber Threat Intelligence (CTI), as a part of a proactive information security program, will become essential for information security. In response to increasingly dynamic threat situations, it is critical for organizations to be able to identify evolving methods and emerging technology trends used by the cybercriminal, and then to continually assess their capability in this regard. Because many organizations don´t have access to internal specialists, they will need to turn to external experts from the CTI sector. Effective cyber security will require knowledge and understanding of the capabilities and intent of threat actors. Who are they? What do they want? What can they do? Organizations will define threat more specifically (i.e. less reliance on vague terms like "vulnerabilities"). We will see an emphasis on threat actors with means, motive, and opportunity being tracked. Understanding motive will become crucial for prioritizing resources.

Cody Cornell, Founder & CEO, Swimlane

"The proliferation of the Internet of Things will exponentially increase the IT workload and transform the way we must conduct security operations management in 2016. An abundance of online devices means more connections to scan for vulnerabilities, monitor for compromises and protect from attacks. With analysts and managers already dealing with thousands of alerts every day, IoT growth will exacerbate the challenges these professionals already face.

Automation will be one of the keys to increasing efficiency in enterprise SOCs. For instance, an automated incident response system can identify and resolve low-complexity, high-volume tasks with little to no human intervention, leaving expert security personnel with more time to handle the more nuanced and complicated issues. That is critical, not only because more devices will create more tasks, but because attacks are growing increasingly sophisticated. Additionally, if that same platform can centralize information from existing security tools, it streamlines operations by limiting the number of tools that analysts use to initially triage alerts. And if the platform can capture processes for standardization and reuse, it further increases productivity by reducing duplicative work."

Alex Brisbourne, CEO, KORE

"2016 will be the 'year of healthcare, agriculture and field service" when it comes to mainstream IoT adoption. High-leverage devices to connect patients to their providers, including IoT-enabled wellness monitors, blood pressure cuffs, blood glucose monitors, scales, pulse meters, and appliances like pacemakers have been growing steadily in use over the past few years; by the time next December arrives, they will be virtually run-of-the-mill as doctors, patients and insurers alike all wake up to the tremendous boon these devices bring at once to quality of care, quality of life and cost-savings.

In addition, sensor-based crop management will achieve its just due this year, with climate and water availability challenges reaching an inflection point over the course of 2015. Products like the SG-1000 Leaf Sensor, PureSense and OnFarm will become household names in the farming community based on their proven ability to use sensor data to increase crop yield, save on resources, and increase drought resistance.

Finally, field service engineering has long been considered a job where people find a high degree of meaning in their work, and I believe the IoT will further elevate the calling for those already employed and for net new job seekers in 2016. Connected tools such as smartglasses and watches will simply make the job more fun for travelling technicians, while diagnostic sensors placed in the products to be serviced themselves will make field techs more responsive and empower them to reduce equipment downtime and provide faster, almost magical, issue resolution. There's real value in showing up to fix something an owner didn't even know was broken, or was about to break."

Sam Rehman, Chief Technology Officer, Arxan Technologies

"Security regulation will make a meaningful impact for medical and other IoT devices: Regulatory requirements have generally been viewed as helping to drive organizations to meet minimum security standards. However, the overall security effectiveness or impact of regulatory requirements has been nominal. We can expect to see a much more meaningful advancement in the rigor of security requirements laid down by the regulators in 2016. This is partly due to accelerated advancements in public-private threat intel-sharing, and the regulators' acknowledgement of the need to seek out cutting-edge threat data and security best practices from the organizations that are on the front lines of defending against them. For example, in IoT, the FDA is making significant improvements in beefing up minimum security requirements for medical devices, which could otherwise pose grave safety risks to people, care providers, and medical device manufacturers that depend on their trusted operation. Since the vertical markets are so intimately interconnected, we will also see more teeth behind enforcement of security requirements.

Most important IoT security issues in 2016 will be:

- Cryptographic Key Protection
- Mobile application code hardening and runtime self-protection
- API protection - hardening the authentication of communications from the API to backend servers that house sensitive data and IP

Advice to IT Security Pros:

- Include run-time application self-protection into your IoT mobile apps to protect your brand and your customers
- Don't wait for security regulations before embracing IoT and mobile - harden application code before your apps are released into the wild and become susceptible to risks such as reverse-engineering and tampering"

John Horn, CEO, Ingenu

"The 2G sunset is going to cause more industry chaos than anyone expects. The sunset has already started, and organizations all think they have plenty of time to transition their IoT strategy beyond 2G. They don't. Cellular technologies such as 3GPP LTE won't materially be realized until at least 2020. When you look at historically about how long it takes for all of the pieces to be pulled together for a new network standard, event 2020 may be optimistic.

We'll begin to see a series of "strange bedfellows" as partnerships emerge to help the growing demand M2M / IoT is putting on networks. Tremendous strides forward in battery technology will extend battery life up to 10 years and beyond. This is becoming increasingly critical, as companies want to "set it and forget it" as much as possible. LPWA-type networks will prove a strong competitive force to cellular as networks are built out and traffic demands increase.

Smart City initiatives will continue to grow as municipalities connect the dots, and we'll see at least one Smart City initiative emerge in 2016 that will set a high bar for others to follow."

Amit Rahav, VP of Marketing and Business Development, Secret Double Octopus

"For the IoT to be successful on a global basis, companies will need to implement security measures far different than those that are most commonplace today. We need to rethink authentication, moving away from certificate authorities to allow scale, and encryption, as many of the sensors necessary to gain value from the IoT aren't powerful enough to allow for advance encryption keys."

Marty P. Kamden, CMO, NordVPN.com

"While facing the major transformation of our daily lives because of IoT, we are not completely ready to face related security issues. Since IoT networks will significantly grow in 2016, privacy and security issues related to web-enabled devices will mirror this change. For example, in August of 2015 hackers remotely seized control of over a million Chrysler automobiles, showing ability of having the full control of the cars – activating the windshield wipers, turning the radio and air conditioning on or disengaging the car's transmission. To start tackling increasing online security threats, there are simple security measures that every Internet user should learn about, one of them being VPN (Virtual Private Network). VPNs will be increasingly popular in 2016 as security and privacy issues online will become more prominent, encouraging people to start encrypting their devices' online data, securing transfer of sensitive data, etc. NordVPN, one of the most advanced VPN service providers on the market, 256-bit AES encryption, is available on 6 devices on one account and has zero log policy."

Ian Worrall, CEO, Encrypted Labs, Inc.

"The Blockchain has the ability to transform business similar to the Internet. With IoT, a major issue inhibiting its growth is how to manage the vast amount of data that will be stored around it. I think the answer to this is by leveraging distributed system technologies such as permissioned-server networks (Private Blockchains) or maybe even utilizing the Bitcoin Blockchain. A key aspect of this is inter-corporate collaboration between the networks of big data companies. This is crucial because the larger a single datacenter (one company) becomes, the harder it is to manage & secure. To do so efficiently it would involve (in some cases) competitors working together. This not only facilitates the management of this data, but secures it more effectively through distributed storage encryption. The companies willing to collaborate will succeed, while those overly competitive to control the space will inevitably fail long-term and short-term are impeding industry growth."

Nav Dhunay, CEO, Ambyint

"I expect to see integration of IoT and Big Data applications continue to gain momentum throughout 2016 with adoption within particular industries, such as oil and gas, accelerating at a higher rate due to the current market conditions necessitating rapid efficiency solutions. I believe that we will see a lean towards the creation of more end-to-end IoT and Big Data solutions for industry, able to not only extract data from machines, but analyze it intelligently and initiate autonomous action to onsite processes in order to seamlessly increase efficiencies and preempt and mitigate future issues."

Jason Sabin, Chief Security Officer, DigiCert

"We'll see hackers using IoT devices to springboard access into enterprise networks where they can cause much greater damage by stealing corporate data of high value. 2016 will feature a major company hacked using this method, which will lead to a greater call for device authentication and encryption to be universally applied for IoT offerings. Unfortunately, we likely may see many of these devices still lacking good security hygiene, such as authentication and encryption, until a data breach raises crosses the pain threshold for users and companies are compelled to enact better security."

Nishant Patel, CTO and Founder, Built.io

IoT adoption in the workplace will still be slow. The problem with IoT in the workplace now is security. And we're not convinced that IoT has solved that potential risk. As it stands now, consumers are willing to take the risk that IoT brings. Whereas enterprise organizations simply can't take that chance when customers' sensitive data is at stake. A major shift needs to happen around security and privacy for IoT in the enterprise. 2016 looks to be the year with big developments afoot.

Move over IoT - it's all about IoA in 2016. For the past few years we've talked a lot of about the Internet of Things (IoT). Its "Things" is actually a misnomer and diminishes what's actually happening with technology across every industry. If you think about it, you can't release a product without an API anymore - be it hardware or software, anything with a digital heartbeat MUST have an API. Traditional integration will start to become irrelevant as integration moves to the cloud and APIs become table stakes. Hence, 2016 won't be the year of IoT, it'll be the year of the Internet of APIs (IoA)."

Dr. Davor Sutija, CEO, Thinfilm

"The rise of printed electronics - paper-thin sensors - being integrated to everyday objects such as food, medicine and clothing opens a new opportunity for retailers to engage with consumers through NFC-enabled smartphones. 2016 will see more consumer brands invest in technology such as printed electronics to not only leverage its capabilities to engage with consumers, but maintain control when it comes to monitoring inventory. Printed electronics will play a role in creating the kind of connectivity that will allow retailers and consumers to communicate well beyond purchases."

Jim Heppelmann, CEO, PTC

"Industrial companies will continue to reimagine the relationship between the Internet and their products (things) and how they can best apply those concepts to their business today. Smart, connected products present many challenges— particularly around data and security— that can be disruptive to an organization. The companies that will succeed in 2016 will be able to navigate these challenges and the product and organizational transformations that are required to take advantage of IoT innovation. Augmented reality technology will also start to play a larger role and will unlock new possibilities in the design, monitoring and control of industrial products."

Szymon Niemczura, CEO and Co-founder, Kontakt.io

"Smart, connected devices are already transforming our world. Among other devices, we're seeing more and more deployments of 5,000, 10,000, and even more beacons throughout the US, EU, and APAC territories, and they're becoming involved in increasingly sensitive elements of business. When beacons were all new and relegated more to the status of a promising toy than something that a serious company would use for mission-critical components, this approach didn't carry much risk. Innovators are generally too in love with the potential of new technology to worry about the threats to it. This year will change it. The IoT security will be brought to light as a serious topic that our maturing industry needs. The companies which will offer end-to-end solutions will do both -- win customers and lead IoT revolution."

Robert Golightly, Execution Systems Product Marketing, AspenTech Manufacturing

"Modern process manufacturing is an ecosystem of interconnected software and hardware that helps companies optimize plants and achieve operational excellence. In 2016, oil, gas and chemical firms will increasingly use data visualization and analytics software to transform the vast amounts of information generated by plants into operational intelligence. The more that is uncovered, the more that can be discovered, enabling manufacturers to efficiently resolve operational issues, adapt quickly to dynamic conditions. and remain profitable in a changed energy pricing environment globally."

Trevor Daughney, EVP, INSIDE Secure

"IoT device makers are realizing that they need to secure IoT devices to protect their reputations and customers. In 2016, IoT device manufacturers will pivot from asking 'why is security needed' to asking 'how do I implement security.' They will look to control data access and protect data at-rest, in-motion and in-process using a combination of software and hardware security measures."

Walid Moneimne, CEO, Aspenta

"A key requirement for IoT market will be the ability to deploy solutions internationally. That means that any connected device-whether it's a smart watch or connected car or a manufacturing solution-will need to be designed and developed as a global product, including affordable connectivity."

Tom Fountain, CTO, Pneuron

"With key functionality and security disciplines still evolving, industrial enterprises will focus on "internal" applications where demonstrable value will be critical to validating the investment and ROI thesis of IoT. Specifically, machine-to-machine sensor feeds, predictive analytics and prescriptive response planning will begin to revolutionize maintenance operations. In these areas, existing costs are extremely well-known and ripe for an analytical assault that transforms parts stocking, technician training, staffing and deployment. This validated operational value will provide a robust platform for a broader Industrial IoT strategy and investment for high value "external" use cases that target customer and partner operations."

Sudip Singh, SVP, Global Business Unit Head, Engineering Services, Infosys

"Design Thinking will align IoT with business objectives: In 2016, businesses will stop chasing the colorful rainbows of interesting IoT use cases and instead narrow down to business cases that deliver results. We've been seeing enterprises getting carried away with IoT as a technology and not focusing enough on the business case. Design Thinking will help overcome this by fundamentally focusing on problem definition rather than problem solving. A design thinking approach facilitates the focus on business outcomes and objectives and then helps build an innovative path to achieve the objective. IoT as a technology is disruptive, whether it is the way business models are changing, products being offered as a service, or products evolving more rapidly."

Open Platforms will drive success in IoT: IoT needs are very diverse as each use case is unique and requires customization. To streamline this process, platforms must be extensible and flexible in nature. Even Commercial off-the shelf (COTS) platforms from vendors are deployed as open platforms with APIs for enterprises to develop industry-specific solutions without depending on vendor professional services or system integration services. This model is more scalable, as the IoT requirement is vast and wide, so much so that a single vendor will not be able to address with scale."

Photo credit: Thomas Nilsson via Flickr

Kong Yang, Head Geek, SolarWinds

"With virtually everything now seemingly being connected in some way to the Internet, there's a broader pathway than ever to malicious access to potentially sensitive data. Not only that, but IoT opens the door wider for digital attacks that extend into the physical world. Gartner recently stated that "by year-end 2018, 20 percent of smart buildings will have suffered from digital vandalism" (e.g. plunging buildings into darkness and defacing digital signage). These attacks may seem like nothing more than a nuisance at the moment, but the recent and memorable hacking of a Jeep on the highway put the potential safety threat into context as the lack of protection and security was publicly demonstrated. In 2016, the race to get ahead in the industrial IoT game will coincide with more and scarier attacks leveraging connected "things" as the mechanism to affect worker and facility safety. Whether it be the safe operation of Internet-connected plant infrastructure such as motion control being overridden; shipment or commercial vehicle location tracking being compromised for nefarious purposes; or breaching a critical hospital device, such as the reports that drug pumps used in the UK can be hacked and controlled or the possibility that Bluetooth-enabled defibrillators and temperature settings on blood and drug storage units could potentially be commandeered, all could lead to life threatening outcomes and highlight as the dangerous lack of security surrounding IoT that will make the need for human intervention and better cloud, data and network management a much higher priority in the coming year."

Patrick Salyer, CEO, Gigya

"The importance of the IDoT will eclipse fascination with the IoT. Cisco projects that the Internet of Things (IoT) is a $14 trillion revenue opportunity, making smart, connected products—and the technologies that make them tick— drivers of huge new growth opportunities. However, according to Gartner, Inc, "Managing identities and access is critical to the success of the Internet of Things," making the Identity of Things, or IDoT, the new focus of the IoT. The IDoT is based on the principle that all entities in the IoT ecosystem—including people, apps, services and connected things—have identities comprised of identifiers and their attributes, and that those identities define relationships between every entity. Managing the data that flows between these identities requires an identity management solution that unifies every entity in the system - a core requirement for businesses looking to capitalize on the IoT in 2016."

Kevin Walsh, VP Marketing, Bsquare

"2016 will be the year actual business IoT deployments accelerate. Not unlike any new technology, there is a propensity among suppliers to rechristen products and/or services they already offer using terminology associated with that new technology. Hence it might appear that the business-oriented IoT market is already going gangbusters when in fact it's still in its infancy. This tendency is understandable and, in some cases, not completely without merit but what is truly interesting for businesses are complete systems where intelligent devices generate data that is captured by enterprise systems in order to automatically drive desired business outcomes. This, more than anything else, is why IoT is not even remotely the same as M2M. For possibly the first time, 2016 will mark the beginning of complete, large scale IoT systems that directly and automatically link devices with business outcomes."

Kuruvilla Mathew, Chief Innovation Officer, Ness

"Wearables will start seeing significant improvement in the analytics of what the devices provide, including more fine grain data that will help in providing a reliable overall health picture of a consumer. Health insurers will start to move towards comprehensive wellness programs and offer benefits/ credits to healthy insureds. Nearables will make significant inroads into all areas with retailers, hospitals, healthcare, public transport, banking institutions and cities reaping the benefits. All the data that is being collected will be monetized for use across businesses. The data from nearables will be valuable to determine changing behavior of consumers. The analyzed data will provide actionable insights to help businesses fine tune based on behavior."

Dr. Ernest Earon, CTO and co-founder, PrecisionHawk

"In 2016, we expect a dramatic increase in commercial drone sales, which is already a hot topic within the Internet of Things. Over the last two years, several industries have grown increasingly interested in using drones to collect data and make better business decisions. In response to this rising demand in agriculture, we released the Algorithm Marketplace: an app store for users to upload imagery and easily click which output they seek (plant count, plant height, volumetric readings and many others). Additionally, as we continue our partnership with the FAA to test drone flights BVLOS (beyond visual line of site), we may see shifts in federal regulations that could result in additional increases in commercial drone sales in 2016."

Imad Mouline, CTO, Everbridge

"As an increasing number of devices connected to the Internet rely on embedded intelligence to communicate critical information, these devices will not only provide constant monitoring services, but have the ability to apply real-time control as needed. In many cases, intelligent devices can respond faster than a human could. For example, an automatic braking system in car will automatically pump the brake when the car detects it's sliding, rather than alert the driver and wait for him or her to apply the brakes. Despite the increase in networked, intelligent, and automated systems, the need for human intervention will remain. In an automated environment, decisions may set off chain reactions of cause-and-effect, leading to unintended consequences, and as processes speed up, critical decisions increasingly require expert level opinion."

Sukamal Banerjee, EVP, Engineering & R&D Services, Head of IoT Business, HCL Technologies

"The intersection of employees, data and technology enabled intelligent machines is creating fundamental shifts in enterprise business models, leading to not only increased productivity and efficiency but also opening a plethora of new revenue opportunities for companies. Businesses will compete on their ability to deliver quantifiable results in real time that not only adds incremental value but brings unconventional growth that matters to their customers. Successful IoT implementation will require much more accurate predictability and deeper understanding of customer needs. Industries that currently operate in isolation will need to redraw their boundaries to form a connected ecosystem and then collaboratively provide the desired customer experience."

Bart Schouw, Director of Industry Solutions, IoT, Software AG

"If today is cloudy – tomorrow is foggy. Right now, we are all busy to adopt cloud. But if we would have to talk about cloud in terms of the eighties we would call it timesharing on something that represents a distributed mainframe. With the processing capacity still growing and the need for intelligent things to operate independently even if they are disconnected from the central brains, we will see intelligence and decisioning power moving to the edge we will call this fog-computing. Say hi to your digital twin. On an abstract level you can describe the movement of IoT as the need to create digital twins of things that are present in the physical world. The first step is to create a true as possible copy (life-like) using real-time data to have an up to date view as possible. We will call that the digital twin. The next step will be to add more intelligence to the digital twin, we will give it attributes that the real physical thing doesn't have like an agenda. Allowing it to take part into real world processes without the intervention of a humans."

John Marchiando, VP of Business Development, Grid Connect

"GE Software (Predix) will be the platform to watch. GE is turning itself from a traditional manufacturing company into a digital industrial company, driven by data. Their investment in GE Software, in San Ramon, California, is a significant step in that direction. Predix, for example, is a cloud service that's built for the industrial enterprise, not something that was originally developed for the commercial enterprise and "shoehorned" into the industrial space. Their key areas of focus are sensors, data analytics, predictive analytics, energy efficiency, user interfaces, mobile technologies and transportation logistics, all key areas in the industrial space and in line with GE's core businesses. They employ over 800 software engineers in this business, which didn't exist until 2011."

Smart city applications will begin to take off. Many new applications are becoming commonplace in cities, like smart parking (understand where cars are parked, for example), smart water (monitoring for chemicals in the water supply or detecting where water is present), smart environment (measuring for CO2 emissions to understand where companies might be polluting the air). These are allowing cities and municipalities to improve congestion, traffic, access to parking, their water supply and possible sources of pollution."

Kellman Meghu, Head of the America's Security Architects, Check Point Software

"The Internet of Things is perhaps the number one technology trend that is gaining momentum by the second. As we witness the merging of innovations in the areas of computing and communication, intelligent devices are set to transform human-to-machine interaction, as well as machine-to-machine interaction.

However, with the sheer amount of devices hitting the market, the challenges of securing these items is quickly becoming front and center. With that said, we invite you to shift your perspective for a moment. Most conversations surrounding IoT are limited to consumer technology -- yet the conversation must expand to include the dark underbelly of how these technologies are built, secured and distributed. Beyon the consumer, there are three main areas of IoT that Check Point believes are crucial to secure: 1) Industrial IoT, 2) Workplace Wearables, and 3) Securing the infrastructure of Service Providers.

Devices that connect to each other and over the internet potentially threaten Industrial Control Systems (ICS). Those systems are referred to as critical infrastructure for a reason - they are critical, meaning that society cannot function without them. As businesses require that industries move beyond "intelligent" devices merely as a means of control, they are likely to run into complications as they seek to integrate Industrial IoT into their office - and production - environments.

Wearables in the workplace also pose an interesting security risk. As the employees of your organization bring smart devices (phones, watches, medical monitoring gear, etc.) into the environment, and allow them to connect to the company networks, this could potentially introduce a variety of threat vectors through the network. This is a potentially huge problem.

Finally, what are the service providers doing to secure the devices or appliances they manufacture? Are companies who produce "smart refrigerators" and "smart toasters" taking an active stance in making sure their own environments - be it datacenters, cloud environments or networks - are secure before the devices they support are installed into millions of homes? Again, it's not about the devices themselves, but about the integrity in manufacturing and security the environments in which they operate.

By itself, the Internet of Things is not the problem. The main risk is its potential - and that is to open gateways within an organization's borders. Having more gateways to protect puts further stress on security teams and technology. Ultimately, the market will demand technology that is intelligent and powerful enough to prevent and combat these threats at the very source."