G00291252

Top Strategic Predictions for 2016 and Beyond: The Future Is a Digital Thing

Published: 2 October 2015

Analyst(s): Daryl C. Plummer, Van L. Baker, Tom Austin, Charles Smulders, Jim Tully, Ray Valdes, Adam Sarner, Kristin R. Moyer, Frances Karamouzis, Whit Andrews, Jay Heiser, Sylvain Fabre, Angela McIntyre, Don Scheibenreif, Karen A. Hobert, Jenny Sussin, Richard Marshall, Rob Smith, Martin Kihn, Magnus Revang, Adrian Leow, Jason Wong, Diane Morello, David Furlonger, Kenneth F. Brant, Helen Poitevin

The dramatic rise of smart machines and autonomous devices is driving radical shifts in business practices and individual behaviors. Enterprises and individuals face the urgent need to define and develop harmonious relationships between people and machines.

Key Findings

- The relationships between machines and people are becoming increasingly competitive, as smart machines acquire the capabilities to perform more and more daily activities.
- "Smartness" is now everywhere in the work environment, with consequences that are difficult for enterprise decision makers to foresee.
- The Nexus of Forces is evolving and expanding into an entirely new set of scenarios.

Recommendations

- Use Gartner's predictions as planning assumptions on which to base your strategic plans.
- Evaluate the near-term flags that indicate whether a prediction is trending toward truth or away from it.
- Position predictions with longer time horizons as having a lower probability of coming true than those with shorter time horizons.

Table of Contents

Strategic Planning Assumptions

By 2018, 20% of all business content will be authored by machines.

By 2018, 6 billion connected things will be requesting support.

By 2020, autonomous software agents outside of human control will participate in 5% of all economic transactions.

By 2018, more than 3 million workers globally will be supervised by a "roboboss."

By YE18, 20% of smart buildings will have suffered from digital vandalism.

By 2018, 50% of the fastest-growing companies will have fewer employees than instances of smart machines.

By YE18, customer digital assistants will recognize individuals by face and voice across channels and partners.

By 2018, 2 million employees will be required to wear health and fitness tracking devices as a condition of employment.

By 2020, smart agents will facilitate 40% of mobile interactions, and the post-app era will begin to dominate.

Through 2020, 95% of cloud security failures will be the customer's fault.

Analysis

What You Need to Know

Gartner's top predictions for 2016 and beyond continue to offer a look into the digital future, a world driven by algorithms and smart machines, where people and machines will need to define and develop harmonious relationships. These predictions help our clients understand the radical changes they face in the digital world.

Those changes are coming fast. We predict, for example, that in 2016 spending on new Internet of things (IoT) hardware will exceed $2.5 million *a minute.* And, as mind boggling as that number is, it pales in comparison with the corresponding prediction that, by 2021, 1 *million* IoT devices will be purchased and installed *every single hour.* That level of density of deployment and use will present dramatic challenges to enterprises and IT organizations that need to manage and track IoT activities.

The changes that are coming extend far beyond the IoT. The increasingly smart, autonomous nature of machines means that we're seeing the beginning of "robos" rising — the worldwide spread of autonomous hardware and software machines to assist human workers in practical scenarios.

Robowriters are now creating business content. Roboagents are conducting ever more critical economic transactions. And robobosses are emerging that will eventually supervise significant portions of the workforce. The rise of robots is a serious challenge, but it's also an opportunity to increase the use of smart machines to develop more effective work strategies.

The "robotrend," the increasing practicality of artificial intelligence, and the fact that enterprises and consumers alike are now embracing the advancement of these technologies, is also driving the development of risky scenarios. The risk to human jobs when roboworkers enter the workforce in volume is obvious, but it's balanced by the need for talent capable of developing smart systems and autonomous processes. Companies like GE, GM and IBM see Silicon Valley talent as an inducement to move more of their operations to those locations. The future will belong to the companies that can create the most effective autonomous and smart software solutions. So in the near future, at least, jobs are more likely to be created than to be eliminated on a massive scale.

The real risks are less obvious. As digital capabilities are included in more and more systems, the ability of unscrupulous individuals — including software-based thieves — grows. Digital smart buildings are being attacked as more access to software systems means more control surfaces will become vulnerable. Digital signage; heating, ventilation and air conditioning systems; and even lighting and environment controls are subject to attack, especially in industries where few policies for detecting and preventing hacks on these kinds of systems are in place. The savvy digital officer must now contend with risks that fall outside the normal assumptions of risk related to computing technologies.

This year's 10 seemingly disparate top predictions are more closely related than they might seem at first glance.

Among the high-level trends that emerge from these predictions are:

- **The relationships between machines and people are moving from the cooperative to the co-dependent to the competitive:**

  In last year's predictions, we stated that the world was rapidly moving to a future in which machines and humans would be co-workers, and possibly even co-dependents — and this is now a reality. We're seeing an increase in the use of autonomous and smart machines, and in the ability of those machines to depend on human partners. Forty-seven percent of devices will soon have the necessary intelligence to request support. Things everywhere, from connected engines to connected prostheses, will be requesting support from humans and human-managed businesses. Vending machines, vacuum cleaners, printers, air fresheners, security cameras, parking meters, soap dispensers and aircraft are just a few examples of things that will be asking for repair. The next frontier is a world where machines compete with people to perform more and more daily activities.

- **"Smartness" is being applied across the entire fabric of the work environment:**

We need to be asking ourselves, "How smart is smart enough?" when it comes to software systems and devices. When devices become smart enough to go beyond simple autonomous behavior, to behavior that is less predictive, we open the door to unexpected — and potentially unwanted — results. The prevalence of metacoin platforms driven by software algorithms, for example, allows the emergence of a fully programmable economy operating beyond the control of centralized institutions or even governments. Will this lead to software agents acting as robothieves, making unauthorized economic transactions? Will the rise of smart machine instances in the workforce drive a psychological wedge between businesses and their employees, making them feel increasingly like parts of an all-encompassing business machine? These are questions that, while not yet fully answered — and perhaps not fully answerable, are examined implicitly as part of our predictions on the future of smart machines.

- **The Nexus of Forces is evolving and expanding into an entirely new set of scenarios:**

  Security responsibility, personal identification and the evolution of the post-app era are three areas where we see the converging factors that Gartner has identified as the Nexus of Forces — social networking, cloud computing, mobile communications and information — continuing to evolve. As security concerns take center stage for digital customers, it is becoming clear that security is everyone's problem. We predict that cloud security will evolve to become more of a customer maturity issue than a provider issue. We allude to the fact that password identification will no longer be enough, and much of our personal "image" will become our digital signature. We also state categorically that mobile apps are not the final word when it comes to the way individuals interact with businesses. These three issues expose us to the notion that the maturity of cloud and mobile, and the need for more effective approaches to security, are now becoming core value propositions for business.

Gartner's top strategic predictions continue to offer a provocative look at what might happen in some of the most critical areas of technology evolution. Even more important, they help us to move beyond thinking about mere notions of technology adoption, drawing us more deeply into issues surrounding what it means to be human in the digital world. Whether one is a customer, a business or an investor, these predictions will be useful for capturing the interest of strategic thinkers and fueling the excitement of tactical decision makers.

Strategic Planning Assumptions

By 2018, 20% of all business content will be authored by machines.

Analysis by: Karen A. Hobert and Martin Kihn

Key Findings:

- Technologies with the ability to proactively assemble and deliver information through automated composition engines are fostering a movement from human-generated to machine-generated business content. Information based on data and analytics can be turned into natural-language writing using these emerging tools. Business content types — such as shareholder reports, legal documents, market reports, press releases, articles and white papers — are all candidates for automated writing tools.

- Consumer-centric paradigms are likewise driving the application of intelligent systems to the creation and distribution of personalized marketing content that is used to attract and retain consumers (see "Market Guide: Digital Personalization Engines").
- One of the earliest and most compelling use cases for machine-generated content is occurring already in marketing and advertising. There is ample evidence that greater message and image personalization leads to better results (for example, 40% higher engagement rates on a website and 2.3 times better response to digital advertising, according to recent benchmarks). The problem is one of scale: If a marketer has thousands (or millions) of prospects and customers, it is not possible for humans to generate thousands (or millions) of different messages.
- Today, we are seeing machine-generated content in a few limited applications:
  - Article and documentary copy, layout and publication based on data feeds (often in real time) and analysis.
  - Recommendations for products on e-commerce sites and email, where machines generate basic headline copy and layout, including offers.
  - Layout and image arrangements on websites through predictive content algorithms.
  - Machines writing basic paid search ad copy.
  - Dynamic creative optimization on sites and ads, where machines create and test versions based on known parameters and templates (which are created by people).
- Improvements in machine learning, data integration and predictive analytics apps for all areas of business content are combining to inspire a new class of solutions — such as Automated Insights and Persado — that provide machine-written verbal treatments and machine-derived imagery for personalized messaging at very high volumes. For example, Automated Insights has already been employed to robowrite thousands of reports for fantasy football newsletters based on fairly rigid templates, and an intrepid reporter in Southern California has configured a system to automate the writing of basic near-real-time earthquake dispatches based on seismic and other data. These examples represent an early, primitive stage of a rapidly developing set of solutions.
- Automated composition technologies offer a broad range of benefits, including:
  - Contextualized content (automatic and contextualized content creation based on the reader's location, activities and device, to deliver the right content to the right person at the right time).
  - Authorship velocity (just-in-time document generation and authoring through real-time analytics and monitoring of information feeds, which can be faster than human authorship).
  - Content quality and consistency (improved quality, consistency and format of business content, through automated editors that provide natural language and translation services based on templates and rules).

Market Implications:

Content management vendors are adding better content composition and analytic capabilities to their systems. Improved capacity to support different device types, diversity of information formats, and real-time monitoring and analysis of content sources are offering customers more efficient ways to assemble information into new content.

Solutions that combine the ability to find, analyze and assemble data into formats that can be read in natural language will improve both the speed and the quality of business content delivery. Personal assistants such as Apple's Siri and Microsoft's Cortana — as well as IBM Watson, with its cognitive technology — provide richer and more interactive content. Drones, sensors, wearables and cameras will create huge volumes of data that needs to be accessed and assimilated into understandable content.

Today, the applications are text-based, but dynamic creative advertising solutions for display and video (including Mirriad, SundaySky and Alliant) point to a rapidly evolving space in which image and video personalization is poised for growth.

Near-Term Flags:

- By YE16, more than 10 significant vendors will have commercially available managed services offerings that use smart machines to create written content and basic design elements for enterprise content, websites, email, and some mobile applications.
- By YE16, two major advertising holding companies will have placed a hiring freeze on copywriters and make significant investments in robowriting solutions.

Recommendations:

- Evaluate emerging vendors to identify automated content generation services (for example, article writing or Web content generation) that your enterprise might want to use today.
- Review content management vendor roadmaps to determine their ability to offer automated content generation or integration into systems that generate natural-language content.
- Consider content management vendors' analytics capabilities, current or planned, and identify ways they might be useful for automated content generation.
- Evolve your marketing segmentation and targeting disciplines to handle many more microsegments.
- Improve your A/B and multivariate testing discipline to better define success for different prospect groups.
- Review current enterprise plans for new devices, wearables, scanners and attendants that might produce new data formats and metadata, and determine whether the information they produce could or should be leveraged for autogenerated business content.

- Conduct an exploration of jobs (or roles) that could be augmented with automatic content generation capabilities, and especially where it can provide more value to customers.
- Cultivate a mind and process shift among creative team members and agencies toward more modular and template-based creativity (that can be manipulated by machines as creative "elements") rather than finished products.

Related Research:

"Hype Cycle for Content Management, 2014"

"Hype Cycle for Digital Marketing, 2015"

"Top 10 Strategic Technologies — The Rise of Smart Machines"

"Market Guide: Digital Personalization Engines"

By 2018, 6 billion connected things will be requesting support.

Analysis by: Jenny Sussin, Jim Tully, Kristin Moyer and Don Scheibenreif

Key Findings:

- Customer service organizations are already capable of taking support requests from connected things (for example, security systems that alert a security company that an alarm has been tripped).
- The number of connected things is set to grow exponentially. In Gartner's IoT forecast, we estimate that, by 2020, more than 35 billion things will be connected to the Internet (see "Forecast: Internet of Things, Endpoints and Associated Services, Worldwide, 2014").
- We also estimate that 47% of devices will have the necessary intelligence to request support. Things everywhere, from connected vehicle engines to connected prostheses, will be requesting support from humans and human-managed businesses. Vending machines, vacuum cleaners, printers, air fresheners, security cameras, parking meters, soap dispensers and aircraft are a few examples of things that will be asking for repair, refill and proactive maintenance in every industry — whether business-to-business (B2B) or business-to-consumer (B2C) — and every geography. Many of these requests will be for very simple actions, such as the need to replace or recharge a battery, and most will require human intervention.
- As the computational intelligence of Internet-connected things increases, so will their ability to request support — and to receive it automatically. Examples we see today include medical devices from Biotronik that allow doctors to monitor patient health for remote evaluation, and Tesla electric vehicles that call the company to request corrective software downloads, independent of their human owners.

Market Implications:

In the era of digital business, when physical and digital lines are increasingly blurred, enterprises will need to begin viewing things as *customers* of services — and to treat them accordingly. They will need to develop mechanisms for responding to significantly larger numbers of support requests communicated directly by things. They will also need to develop strategies for responding to them that are distinctly different from traditional human customer communication and problem solving.

Responding to service requests from things will spawn entire service industries, and innovative solutions will emerge to improve the efficiency of many types of enterprise.

Things will become more autonomous as technologies evolve, and as we learn to trust them. In a number of scenarios, things (as customers) will have the ability to choose between alternative service providers and to negotiate prices and other terms.

Customer service capabilities for managing support issues that are largely algorithmic and objectively driven will allow for less human-agent-based support, and more M2M-based support. This will make more efficient customer support possible, but will also negatively impact the ability of enterprises to differentiate on the basis of customer experience. Customer experience requires subjectivity — perceptions and feelings — while things deal purely in the objective.

Near-Term Flags:

- By YE16, connected car subsystems will exceed 600 million units.
- By YE17, the number of connected health and fitness devices will exceed 580 million units.

Recommendations:

- Initiate collaboration with the chief digital officer, chief strategy officer and other key stakeholders to explore the strategic implications of things as customers requesting service.
- Develop scenarios, such as business moments, that envision how things that you deploy to customers or that are present in your customers' locations could impact how you approach customer service.
- Examine your customer journey maps and determine how a thing might intervene or act on behalf of your human customers.
- Think specifically about how your customer service functions might be impacted in these scenarios
- Build intelligent devices into your technology innovation pipeline.
- Begin to explore partnerships with companies that are building intelligence into things.
- Learn how the technology works, consider the systems that are needed for coordination and orchestration, and think about how your enterprise will fit in that ecosystem, especially with regard to customer service.

- Challenge your current customer service technology partners to understand how they will help you adapt to this future.

Related Research:

"Maverick* Research: When Things Become People"

"Internet of Things Scenario: When Things Negotiate"

"Internet of Things Scenario: When Things Become Customers"

"Mass Adoption of the Internet of Things Will Create New Opportunities and Challenges for Enterprises"

"The Internet of Things and Related Definitions"

"Digital Businesses Will Compete and Seek Opportunity in the Span of a Moment"

By 2020, autonomous software agents outside of human control will participate in 5% of all economic transactions.

Analysis by: Magnus Revang, Ray Valdes and David Furlonger

Key Findings:

- Algorithmically driven agents are already participating in our economy. However, while these agents are automated, they are not fully autonomous, because they are directly tethered to a robust collection of mechanisms controlled by humans — in the domains of our corporate, legal, economic and fiduciary systems.
- The use of blockchains, of which bitcoin is but one implementation, has the potential to deliver disruptive change, as cryptocurrency-based technologies become more widely adopted and evolve to powerful decentralized platforms supporting diverse scenarios for value exchange.
- Metacoin platforms using the trustless blockchain mechanism for a distributed global ledger of transactions will evolve to include fully embedded programmability of objects.
- Algorithmically driven entities on next-generation metacoin platforms will be able to hold, accumulate and spend money. They will also be able to enter into contracts involving conditional payments.
- Entities on these globally distributed platforms can adapt, replicate, evolve and spawn new autonomous agents.
- The result of the prevalence of metacoin platforms will be the emergence of a fully programmable economy operating beyond the control of any single centralized institution or government. It is the metacoin platform that enables automatic enforcement of conditions in a fully distributed and untrusted environment.

- Autonomous software agents will hold value themselves, and function as the fundamental underpinning of a new economic paradigm that Gartner calls the "programmable economy."
- By design, humans cannot control these entities, once the fully distributed autonomous software agents are "set free" — running live on the blockchain ledger.
- The programmable economy has potential for great disruption to the existing financial services industry. We will see algorithms, often developed in a transparent, open-source fashion and set free on the blockchain, capable of banking, insurance, markets, exchanges, crowdfunding — and virtually all other types of financial instruments.

Market Implications:

- A fully evolved programmable economy is a tectonic change disrupting the seemingly unassailable institutions of both government and the global financial industry. The implications of the blockchain for the economy are comparable to those of the Internet for information.
- Autonomous software agents will compete with common offerings from financial institutions — like bank accounts, exchanges, markets and insurance — while being vastly more transparent. They will likely force financial institutions to adopt new revenue streams as old streams are displaced.
- Because these autonomous agents live in a fully distributed environment, they are effectively ungovernable, creating challenges for governments and placing the fundamental mechanisms of ownership and taxes under pressure.

Near-Term Flags:

- By YE16, 80% of the world's largest banks will have initiated blockchain-based projects (by YE18, 80% of these projects will have been terminated, due to the immaturity of first-generation technology).
- By YE16, at least three national governments will have announced that they will use blockchain technology as an authoritative record for significant transactions, such as land ownership.
- By YE17, at least one major financial institution will announce that it is redesigning its business model and core systems around the use of a blockchain.
- By YE18, a bitcoin alternative or derivative, capable of running Turing-complete software code, will have surpassed bitcoin in total value.
- By YE19, 5% of the value of economic transactions in the world will involve blockchain technologies.

Recommendation:

- CIOs in the financial industry should immediately form teams to build blockchain competencies, monitoring and analyzing the implications of these technologies on the business. Blockchain technology is difficult to grasp fully — because it involves elements of cryptography, peer-to-peer communications, game theory and advanced economic theory — and it therefore requires a multitalented team.

Recommended Research:

"Maverick* Research: In a Post-Bitcoin World, Metacoin Platforms Enable the Programmable Economy"

"Hype Cycle for the Programmable Economy, 2015"

"The Future of Money Is the Programmable Economy, Not Just Bitcoin"

"Cool Vendors in Web Computing, 2015"

By 2018, more than 3 million workers globally will be supervised by a "roboboss."

Analysis by: Whit Andrews, Frances Karamouzis, Ken Brant, Helen Poitevin, Tom Austin and Diane Morello

Key Findings:

- Supervisory duties are increasingly shifting into monitoring worker accomplishments through measurements of performance that are directly tied to output and customer evaluation. Such measurements can be consumed more effectively and swiftly by smart machine managers tuned to learn based on staffing decisions and management incentives.
- The "gig economy" — where workers compete for short-term contracts rather than working for a salary — is making a large amount of talent available to enterprises in structured, task-granular formats. Talent can be sourced, selected and engaged in an automated fashion.
- Robobosses will depend on data directly derived from worker performance and on their own ability to derive insights from that data that a human might not reach, or might reach less quickly.
- Smart machine technologies and services are available today in the commercial market. Smart machines demonstrate certain key attributes:
  - They deal with high levels of complexity and uncertainty to form hypotheses based on what they have learned.
  - They test those hypotheses to refine probabilistic conclusions.
  - They have developed a better understanding of task-specific contexts than many industry observers had predicted.

Market Implications:

Robobosses will increasingly make decisions that previously could only have been made by human managers. For example, they will route work and evaluate performance with nuance and flexibility (they will not, however, manage out-of-workflow exceptions, such as the need for compassionate leave, in the foreseeable future).

Business process outsourcers that focus on performance appraisals, incentives and pay will develop smart machine "contract managers" designed to handle measurement and supervision of particular worker classes.

Measurement of worker performance will become even more granular as smart machines become the primary means of analyzing performance. Activities and events that would be far too minuscule for human managers to track — for example, the angle at which a plate is presented to a diner, the speed at which a driver turns a corner, or the percentage of completeness that a smile reaches in front of a VIP customer — will be fodder for machines capable of uniquely powerful and granular micromanagement.

Reactions to such measurements will become equally deft and individual. Smart machine managers will present servers to diners based on optimized personality and interaction profiles. Technicians will be assigned to tasks at which they uniquely, but almost invisibly, excel. Gig economy freelancers will participate in efficient work chains driven by minutely measured processes.

Near-Term Flags:

- A major software vendor or business process outsourcer will release a "worker management" smart machine during 2016.
- Another major services subindustry will face a successful sharing economy disruption (like Uber) in 2017.
- More than 30% of freelance professionals will be selected for work through sharing marketplaces in major labor markets in 2017.

Recommendations:

- Train managers to focus on "human" issues, such as creative leadership, worker relations, and strategic planning. Training must focus less on simply measurable worker behaviors and their correlation. Human managers should be given clear instruction on what they can accomplish that machines cannot. The managers themselves should be measured on worker satisfaction with the company, and balancing of performance metrics against the necessities of living. Human managers may be partnered with smart machine managers in a way that allows them to influence the skills and strengths of the machines.
- Establish fine-grained measurements to allow for the discovery of benchmarks and flags that would not have been detectable previously.

- Correlate several measurements instead of depending on individual measurements. Individual metrics (overall satisfaction with a transaction, for example) must be combined with other metrics to develop a more meaningful picture (this might include an increase or decrease of satisfaction for a given transaction that is measured by comparing it with the previous transaction, or other transactions made at the same time). Individual measurements that are based on fulfillment of particular process steps must be combined with other such steps, and with outcomes, to fuel effective relationship discovery.
- Ensure that smart machine development for management purposes combines the machines' propensity to identify, document and employ new patterns. Smart machine managers will look at data in new ways because of their ability to dispassionately discover previously undetected relationships and correlations, test their hypotheses, and then elevate them to production status.

Related Research:

"Hire the Right Staff to Best Employ Smart Machines"

"The CIO Survival Guide: Your Role in a World of Increasingly Smart Machines"

"Smarter Machines Will Challenge the Human Desire for Control"

"Mandate Investigation of Smart-Machine-Enabled Services to Accelerate Business Outcomes"

By YE18, 20% of smart buildings will have suffered from digital vandalism.

Analysis by: Richard Marshall and Rob Smith

Key Findings:

- Inadequate perimeter security will increasingly result in smart buildings being vulnerable to online attacks.
- Most of these attacks — unlike conventional criminal hacking intended to recover personal, financial or governmental information — will be of purely nuisance value. These exploits will likely happen simply because they are possible, as is the case with physical graffiti and broken windows.
- With exploits ranging from defacing digital signage to plunging whole buildings into prolonged darkness, digital vandalism is a nuisance, rather than a threat. There are, nonetheless, economic, health and safety, and security consequences. The severity of these consequences depend on the target. Unlocking all the secure doors in a building via an unprotected control system may not be important for an office, for example, but would be a severe problem for a prison.

- The digital vandals perpetrating these attacks are likely to be exploring, trying to see what they can do, and are probably unaware of the consequences of their acts. There may, in fact, be no malicious intent, with an attack starting simply as a prank.
- The flexibility and power of smart digital buildings comes with risks, due to the complex, loosely integrated systems that form typical control networks. In 2015, we have seen control hackers take control of cars via their entertainment systems, and the potential risk is more serious for buildings. Cars are systematically designed, integrated and built by a single organization, and are rarely refreshed. Buildings, by contrast, evolve organically over extended periods, with regular renovations, making them more vulnerable.
- Existing systems in buildings are frequently ripped out and new ones put in as technology evolves. Different aspects of the building evolve at different speeds, according to their nature, available budgets and levels of wear and tear. Permanent signage may be replaced with digital displays — often low-cost tablets — at a different time from the building management system. Smart lighting is fitted according to the lampage schedule, and the Wi-Fi and Bluetooth beacons are added to the building by different contractors, but they are all interconnected. If just one contractor leaves an access point on the default password, the entire network may compromised.
- A newly constructed building may be created as a single system, but as soon as a single lamp has been replaced, the system has changed, and if that lamp includes unprotected smart controls, it may offer attack surfaces.

Near-Term Flags:

- By YE16, several major offices will have been disrupted as digital signage has had to be turned off due to obscenities or other inappropriate messages posted on meeting room doors.
- By YE17, a major shopping mall will be evacuated because hackers have turned its cooling system to heating during the summer, and raised the internal temperature of the building until it is unsafe for occupation, resulting in revenue loss for the retailers and possible fatalities of elderly or infirm shoppers.
- By YE17, a school emergency lockdown will be triggered by students breaking into the school's management system.
- By YE18, a national legislative assembly will be shut down for several hours because hackers have turned off the lights in the debating chamber.

Market Implications:

Smart building components cannot be considered independently, but must be viewed as part of the larger organizational security process. Products must be built to offer acceptable levels of protection and hooks for integration into security monitoring and management systems. Certification programs that allow organizations to ensure the correct level of security for their needs during procurement will be required.

Recommendations:

- Ensure that smart building systems come under the authority of the chief security officer.
- Audit all building systems to check for potential security weaknesses.
- Maintain up-to-date architecture and network diagrams that include all connected building components.
- Include digital vandalism in your emergency and contingency planning.

Related Research:

"Prepare for the Security Implications of the Digital Workplace"

"Market Guide for Security Consulting Services, Worldwide"

"Cool Vendors in Mobile Security and IoT Security, 2015"

By 2018, 50% of the fastest-growing companies will have fewer employees than instances of smart machines.

Analysis by: Frances Karamouzis and Magnus Revang

Key Findings:

- Gartner estimated the value of the smart machine "technology" market at $6 billion as of YE14.
- Many of the fastest-growing private companies are using some form of smart machine technology, with limited numbers of employees generating significant revenue.
- Startups and other newer businesses are best-positioned to leverage the cost savings, efficiencies and scalability of smart technologies.

Market Implications:

The capabilities of smart machines are rapidly evolving and converging, and they will drive profound advances in the ability to perform complex tasks. They can support both enterprises and individuals in two important ways:

1. By fully automating tasks and removing human control (for example, via algorithmic trading or "lights out" factories with no on-site employees).
2. By augmenting the cognitive and physical performance of individuals in a manner that feels like an extension of their own abilities (for example, via decision support or wearable technology).

One smart machine technology vendor, for example, reports that its robowriter technology created 1 billion stories in 2014, many of them without human intervention. The inverse — in the form of automated essay grading — is also becoming commonplace. The nonprofit online education platform edX has, for example, introduced a computer system that grades student essays and short answers on exams.

Gartner believes the initial group of companies that will use smart machine technologies most rapidly and effectively will be startups and other newer companies. The speed, cost savings, productivity improvements and ability to scale of smart technology for specific tasks offer dramatic advantages over the recruiting, hiring, training and growth demands of human labor. Some possible examples are a fully automated supermarket, or a security firm offering drone-only surveillance services. The "old guard" (existing) companies, with large amounts of legacy technologies and processes, will not necessarily be the first movers, but the savvier companies among them will be fast followers, as they will recognize the need for competitive parity for either speed or cost. Additionally, there are interesting examples of small numbers of employee driving extensive value. And these companies will then go through a renaissance where new business and operating models for growth are seen as the key to competitive advantage.

Many companies are clearly recognizing these advantages. Gartner recently interviewed representatives of three of the fastest-growing private companies in the world. Each of them was using or piloting some form of smart machine technology, and each had fewer than 150 employees generating $85 to $160 million in annual revenue. Facebook's October 2014 purchase of the messaging platform WhatsApp — $22 billion dollars for a company with only 55 employees — is a particularly dramatic example of this trend, and of a new pattern in valuations.

Smart machine cost structures — for both enterprises and vendors — will change radically over time, leading to different margin structures. Entire industries will be disrupted by new delivery options. There will be a bifurcation, with an enterprises viewed as being potentially in one of two categories: having its core business model significantly disrupted; or being the disrupter or "category killer."

This will be most impactful and interesting for small or midsize businesses (SMBs). In the past, large R&D budgets or expensive efforts (involving large capital expenditures for equipment and scientists) were needed to create value and generate patents and other intellectual property. Now the source of value will be algorithmic business models, and the value of the intellectual property generated. Therefore, SMBs will now have opportunities that never existed before.

There will be major shifts in the vendor landscape, driven by a convergence of product vendors and managed service providers that will offer some type of "business process as a service" using smart machines.

Near-Term Flags:

- By YE16, smart machine technology revenues will surpass $10 billion.
- By YE16, one in five global enterprises will have some experience (either licensed or engaged in a proof of concept) with smart machine offerings.
- By YE16, we will see a fourfold increase in sourcing deals that involve a hybrid ecosystem consisting of employees and smart machines.

Recommendations:

- Include some analysis of use of smart machines in every new business model being considered or evaluated as a strategic imperative.
- Ensure that governance and management of a hybrid ecosystem consisting of employees and smart machines is a new mandated competency.

Recommended Research:

"Mandate Investigation of Smart-Machine-Enabled Services to Accelerate Business Outcomes"

"Sourcing Smart-Machine-Enabled Services Drives Competitive Advantage and Future Patent Revenue"

"Digital Business Innovation With Smart Machines"

"Toolkit: Accelerate Digital Business With a Product Creative-Thinking Workshop for Your Executives"

By YE18, customer digital assistants will recognize individuals by face and voice across channels and partners.

Analysis by: Adam Sarner

Key Findings:

- Promising mobile digital assistant technologies such as Cortana, Google Now, Siri, and Amazon Echo are already tapping into preferences and explicit context through spoken questions and commands, connecting pieces of the buying process, such as need/want assessment, information gathering and evaluation.
- While not having to reach the level of true artificial intelligence, top technologies for customer digital assistants will include facial recognition, voice identification, emotion detection, natural-language processing, and audience profile data.
- Assistants will be trainable and capable of learning from each customer interaction.
- Investments in these technologies from high-profile technology providers such as Adobe, Apple, Google, IBM and Microsoft are increasing, and some technologies are already in use.

Near-Term Flag:

- By YE16, mobile devices (including some wearables) that are already equipped with front-facing cameras and microphones will be the most accessible and adopted devices for customer digital assistants that can identify individual customers by face and voice.

Market Implications:

One possible scenario is where you navigate to an clothing website, and the front-facing camera of your smartphone activates momentarily, and the customer digital assistant not only signs you in and greets you by name, but put picks up where you last left off, regardless of what channel you were using previously. Or you might walk into a store and try on some clothes in the dressing room. Invoke the customer assistant embedded in the mirror by asking it to recommend an ensemble with your preferences, in your size, that is in stock and on sale.

Micro sensors on the tags, or woven into the clothing, inform your assistant what you have chosen. Tell it to bill you from your mobile so that you can skip the check-out line. Multiple levels of authentication have you covered.

The last mile for multichannel and exceptional customer experiences will be this seamless two-way engagement with customers. It will mimic human conversations, with both listening and speaking, have a sense of history, use in-the-moment context, timing and tone, and have the ability to respond, add to and continue with a thought or purpose at multiple occasions and places over time.

After decades of improvements in voice recognition and detection technology — as well as improving face recognition technology from large, high-profile organizations like Adobe, Apple, Google, IBM and Microsoft and others — the technology is now already here, and ready for prime time.

Consider Microsoft's Xbox One and Sony's PS4, two leading gaming consoles that both have the ability (through Kinect and the PlayStation Camera, respectively) to recognize and sign in players by face recognition when they enter a room. Both systems respond to voice commands and all of these capabilities are used in-game. Facial recognition technologies exist in multiple photo storage and editing applications. Barclays Wealth and Investment Management's passive voice security service cuts authentication time in its call center by about 20 seconds, resulting in increased customer experience scores for speed, ease of use and security. Other call centers are using emotion detection capability to discern intent and real-time contextual treatment. Although these technologies have been largely disparate across multiple channels, we see that customers are willing to adopt these technologies and techniques that help them sift through increasing large amounts of information, choice and purchasing decisions. This signals an emerging demand for enterprises to deploy customer digital assistants to orchestrate these techniques and to help "glue" continual company and customer conversations.

Recommendations:

- If your industry is retail, financial services, travel, hospitality or another that has high investments in multichannel marketing, exploit first-mover advantage. Over 90% of companies in these industries cannot seamlessly connect more than three channels together around a buying journey, and a customer digital assistant can start to bridge these disparate channels.
- Consider customer digital assistants as an opportunity for businesses to establish customer-led rules of engagement that will start or improve relationships between company and customer. Digital assistants have the opportunity for an opt-in "pull approach," exchanging relevant

information for the purpose, rather than interruptive engagement or a one-sided data gathering exercise that can be perceived as a privacy threat.

- Begin to pilot and beta test key technologies (natural-language processing, voice recognition, facial recognition and voice identification) on mobile devices where the integrated hardware exists.
- Develop a step-by-step opt-in strategy to establish trust for each capability, demonstrating convenient, high-value use cases.

Related Research:

"Multichannel Marketing Survey Results 2015: Marketers Double Down on Real-Time Strategies"

"How Digital Marketers Will Take Advantage of the Internet of Things"

"Predicts 2015: Digital Marketers Will Monetize Disruptive Forces"

By 2018, 2 million employees will be required to wear health and fitness tracking devices as a condition of employment.

Analysis by: Angela McIntyre, Sylvain Fabre and Adrian Leow

Key Findings:

- Corporate wellness programs are increasingly providing fitness trackers as a way to motivate workers to become more physically active. In the U.S., 100 million workers have access to a wellness program. Providers, including startups such as Limeade and Jiff, enable fitness trackers to be an integral part of goal setting and incentives.
- As heartrate tracking gains adoption, especially during exercise, people are likely to become more accepting of sharing data with wellness program providers, with apps like Endomondo and with online communities such as Nike Fuel.
- Seventeen percent of online adults in the U.S. under the age of 75 currently use a fitness wristband/tracker, as do 10% of people in the U.K. (source: Gartner Consumer Survey data). An increasing number of wearables are able to track heartrate, including smart watches, such as Apple Watch and Samsung Gear 2 Neo, and wristbands, such as the Jawbone UP4 and Fitbit Charge HR. Similarly, sports watches with heartrate tracking, such as the Polar M400 and Garmin Forerunner 225, are used by 6.3% of adults in the U.S. and 8.8% in Germany.
- At least 10,000 elite athletes across 35 countries wear a fitness tracking device as part of their training.
- Catapult Sports provides wearable tracker modules to professional sports teams so that coaches can more effectively manage the training of individual athletes. Likewise, the Adidas miCoach elite team system captures data on an athlete's speed, distance and acceleration

during play, and heart rate. The German team that won the 2014 World Cup trained using Adidas miCoach wearable devices.

- Analysis of data from wearable health trackers could determine whether a worker is likely to fall asleep and send an alert. Fatigue is estimated to be an associated factor in 13% of all truck crashes and 28% of single vehicle truck crashes annually.
- For firefighters, the single largest cause of injury, resulting in 45% of all deaths, is stress and overexertion. Future physiological status monitoring could make use of wearables, such as smart shirts, to detect whether the body is under too much stress, as characterized by elevated heart rate, prolonged exposure to high ambient temperatures, dehydration, abnormal respiration or changes in blood oxygen levels. The wearables targeted at consumers are not intended to be used as to save a life, or as medical monitoring devices, and those that are must receive regulatory approval.

Market Implications:

The health and fitness of people employed in jobs that can be dangerous or physically demanding will increasingly be tracked by employers via wearable devices. Emergency responders — such as police officers, firefighters and paramedics — will comprise the largest group of employees required to monitor their health or fitness with wearables. The primary reason for wearing them is for their own safety. Their heartrates and respiration, and potentially their stress levels, could be remotely monitored and help sent immediately if needed. In addition to emergency responders, a portion of employees in other critical roles will be required to wear health and fitness monitors. Such occupations include professional athletes, political leaders, airline pilots, industrial workers and remote field workers.

New services and providers will arise to track the physiological status of workers who are often in hazardous or isolated environments. Mobile personal safety services for field workers and inspectors will use data from sensors to send alerts in case of issues with health and safety.

Smart cities will integrate data from wearables that track the location and health of police officers, emergency medical technicians and firefighters. The appropriate help could be sent to assist them as soon as possible in case of an injury or a health crisis.

Providers of protective gear for emergency responders — like Taser and Globe Manufacturing — will include sensors in garments and helmets to monitor heartrate, detect falls, track location and identify other signs of physical distress.

Near-Term Flags:

- In 2016, 80% of professional teams in North America and Western Europe playing American football, Australian football, football (soccer), basketball and rugby will require their athletes to wear fitness and health tracking devices during training.
- In 2016, 200,000 police officers in the U.S. will be issued wearable devices with activity or health tracking capability.

- In 2017, at least one executive at a top-ranking global enterprise will have to wear a health and fitness monitor as part of his or her contract.

Recommendations:

- Provide a wellness program that includes wearables as a way to encourage employees to lead healthier lifestyles, improve job satisfaction, and increase worker effectiveness.
- Investigate whether data from fitness trackers can confirm whether employees with required physical exercise or rest periods are complying with policy.
- Follow country-specific regulations regarding data privacy and security.
- Consider remotely monitoring the health of employees in hazardous situations or in isolated locations where they could not otherwise get help in a timely fashion in case of an accident or health crisis.
- Respect the privacy of employees wearing fitness trackers by only collecting, storing or viewing information essential to verifying goals or metrics the employee has agreed to prior to data collection.
- Consider having a third party manage the data and analysis, so that the employer does not have access to sensitive employee health data.

Related Research:

"Invest Implications: 'Wearables: New Interactions and New Opportunities'"

"How to Begin Integrating Wearable Devices Into Smart City Governments"

"Forecast: Wearable Electronic Devices for Fitness, Worldwide, 2014"

By 2020, smart agents will facilitate 40% of mobile interactions, and the post-app era will begin to dominate.

Analysis by: Richard Marshall, Van Baker, Adrian Leow, Charles Smulders, Ray Valdes and Jason Wong

Key Findings:

- Apps give smartphone owners access to millions of focused capabilities, but their usage falls within a narrow set of the app inventory on each user's phone.
- Smart agent technologies are emerging that offer new interaction capabilities beyond the simple use of apps on devices.
- Common early examples are virtual personal assistants (VPAs) such as Cortana, Google Now and Siri, but these will broaden to include dedicated agents specific to business tasks, such as Openstream EVA, Viv and Api.ai.

Market Implications:

Passions run strong in the app community as to what apps should and should not be. One of the most fundamental beliefs is that an app should be focused on a simple task that can be completed quickly through an easy-to-use user interface. For simple tasks, this works very well, but most tasks are not stand-alone, but are connected to others. A simple task will get you the answer to a specific question, but it does not link actions. Many activities would benefit from the integration of simple-app-focused tasks to create an automated process, but few mobile app developers have attempted to add this capability. To do so would violate the fundamental belief that an app should focus on a simple task. For a user, swapping between apps means that a simple user experience has suddenly become complex.

Smart agent technologies, in the form of VPAs and other agents, will monitor user content and behavior in conjunction with cloud-hosted neural networks to build and maintain data models from which the technology will draw inferences about people, content and contexts. Based on these information- gathering and model-building efforts VPAs can predict user needs, build trust, and ultimately act autonomously on the user's behalf.

VPAs and other agent technologies have the potential to transform the way work is done and how individuals interact with technology in the digital workplace. Agent technologies will be used to automate complex business processes that can be initiated via a simple conversational interface. Additionally, VPAs will increase employee productivity as increasing numbers of routine workflows are completed without requiring user intervention, allowing employees to focus on more valuable tasks.

Near-Term Flag:

- Look for growing experimentation with smart agents by consumers and your employees.

Recommendations:

- Begin to incorporate the implications of the post-app era, with cloud-hosted smart agents both responding to requests, and acting independently of the user, in your scenario planning.
- Evaluate the capabilities of VPAs and other smart agent technologies to assess how they can be used to increase workforce productivity and enhance customer engagement.
- Assess security and privacy concerns from both the perspective of the employees, and the perspective of the business, regarding potential data leakage.
- Begin development of cloud-hosted services, in areas such as business process management, business intelligence, and customer relationship management data, that can integrate with VPAs and other agent agents to deliver needed information and automate routine business processes.

Related Research:

"IT Strategists Must Prepare for the Rise of Virtual Personal Assistants in the Workplace"

"The Future of Mobile Apps and Their Development"

"Six Mobile App Concepts to Transform Your Business"

"Top 10 Mistakes in Web and User Experience Design Projects"

"Three Underutilized Ways to Improve the Impact of Mobile Apps in Your Organization"

Through 2020, 95% of cloud security failures will be the customer's fault.

Analysis by: Jay Heiser

Key Findings:

- The high levels of concern about cloud service provider security postures have become counterproductive. They are distracting attention from the need to establish the organizational, security and governance processes required to prevent cloud security and compliance mistakes.
- Many enterprises are paying an opportunity cost by allowing unwarranted security fears to inhibit their use of public cloud services that would be more secure, and more agile, than processes they implement within their own data centers.
- The naive belief that SaaS providers are responsible for their customers' security discourages enterprises from addressing the reality of how their employees use external applications. This leads to a misguided leveraging of the power of cloud services, encouraging employees to inappropriately share huge amounts of data with other employees, external parties, and sometimes the entire Internet.
- The failure to take a strategic approach to cloud competency — to put people and processes in place to consistently leverage the security advantages of cloud computing — can easily create workloads that are less secure than those created by traditional computing practices, resulting in unnecessary compliance incidents and data losses.

Market Implications:

Security concerns remain the most common reason for avoiding the use of public cloud services. The various public cloud markets continue to grow at a brisk pace, but enterprises that have come to terms with cloud security are able to make decisions about which cloud services to use more quickly, and with less internal conflict, than those that are still struggling to understand cloud risks.

The diffuse and complex nature of cloud computing will continue to ensure significant and growing opportunities for multiple forms of cloud control planes. ID as a service, cloud application security brokers, cloud management platforms, and other categories of cloud control provide convenient single consoles and management points. These make it possible to ensure common configurations and policies, and monitor and govern user activities, across an increasingly complex virtual enterprise of applications based in infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS) clouds.

Third-party security standards, such as ISO 27001 and SOC2, will become virtually mandatory product features for any enterprise undertaking strategically significant use of a cloud-based service.

recent history has shown that virtually all public cloud services are highly resistant to attack and, in the majority of circumstances, represent a more secure starting point than traditional in-house implementations. No significant evidence exists to indicate that commercial cloud service providers have performed less securely than end-user organizations themselves. In fact, most available evidence points to the opposite. Only a very small percentage of the security incidents impacting enterprises using the cloud have been due to vulnerabilities that were the provider's fault.

During the next several years, the news media will continue to report a growing number of stories about security failures, but only a few incidents a year will be attributable to poor provider technology or practices on the part of a cloud service provider. Most will involve small providers and impact relatively few customers.

The cloud business model provides huge market incentives for cloud service providers to place a higher priority on security than is typical for end-user organizations. Cloud service providers can afford to hire experienced system and vulnerability managers, and their economies of scale make it practical to provide around-the-clock security monitoring and response. The brand-name cloud services use custom platforms, which enables them to avoid the security vulnerabilities that are typical of in-house implementations.

This does not mean that organizations should assume that using a cloud service means that whatever they do within that cloud will necessarily be secure. The characteristics of the parts of the cloud stack under customer control can make cloud computing a highly efficient way for naive users to use poor practices, which can easily result in widespread security or compliance failures.

Most of the enterprises that have implemented cloud application discovery capabilities — typically provided by a cloud access security broker — have discovered that SaaS is being used in ways that expose sensitive data internally and externally.

"Open shares" that can be accessed by anyone on the Internet are a typical customer security vulnerability. The misuse of public cloud services, which inevitably happens if an enterprise does not attempt to exert some control over cloud use, represents a significant increase in the exposure of sensitive data to people inside and outside the enterprise. The secure and regulatory-compliant use of public clouds requires that enterprises implement new organizational policies, develop new skills and undertake new processes.

The growing recognition of the enterprise's responsibility for the appropriate use of the public cloud is reflected in the growing market for cloud control tools. By 2018, 50% of enterprises with more than 1,000 users will use products provided by cloud access security brokers to monitor and manage their use of SaaS and other forms of public cloud, reflecting the growing recognition that, although clouds are usually secure, the secure use of public clouds requires explicit effort on the part of the customer.

Near-Term Flags:

- By YE16, 40% of enterprises with more than 1,000 employees, and 80% of organizations with over 10,000 employees, will have policies and practices in place to approve and track the use of SaaS.
- The number of enterprises with policies against placing any sensitive data in the public cloud will drop to 5% by 2017.
- By YE17, 95% of cloud service providers with annual revenue over $500 million will have at least one formal security evaluation.
- Through YE18, the number of public disclosures of in-house security failures will grow every year, but only one or two incidents a year will be attributed to poor cloud service provider technologies or practices.
- 50% of enterprises with more than 5,000 users will deploy products from cloud access security brokers to control their use of cloud services by the end of 2018.

Recommendations

- Develop and follow an enterprise public cloud strategy. An effective strategy includes security guidance and regulatory compliance guidance concerning acceptable and unacceptable uses of public cloud services.
- Implement and enforce policies on cloud ownership and cloud risk acceptance processes.
- Follow a life cycle governance approach to the use of all cloud services and the processes performed within them. While existing operational practices are usually extended to enterprise applications provisioned within IaaS, most enterprises currently fail to focus the same level of attention on the ongoing operational control of SaaS applications.
- Develop expertise in the security and control of each of the cloud models you will be using. The use of IaaS requires knowledge of virtualization security, and new techniques for network security. SaaS requires knowledge of provider characteristics and the use of cloud access security broker tools. All forms of public cloud require careful control over identity and access.
- Implement technology control planes to address the complexity of cloud diffusion. Enterprise security, identity, compliance, continuity, sourcing, and other IT roles will increasingly use single consoles that enable them to monitor and manage the use of a wide range of externally provisioned services.

Related Research:

"Developing Your SaaS Governance Framework"

"A Public Cloud Risk Model: Accepting Cloud Risk Is OK, Ignoring Cloud Risk Is Tragic"

"Best Practices for Securing Workloads in Amazon Web Services"

"Everything You Know About SaaS Security Is Wrong"

"Hype Cycle for Cloud Security, 2015"

Gartner Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

"Hype Cycle for Content Management, 2014"

"Maverick* Research: When Things Become People"

"Maverick* Research: In a Post-Bitcoin World, Metacoin Platforms Enable the Programmable Economy"

"Hire the Right Staff to Best Employ Smart Machines"

"Mandate Investigation of Smart-Machine-Enabled Services to Accelerate Business Outcomes"

"Multichannel Marketing Survey Results 2015: Marketers Double Down on Real-Time Strategies"

"Invest Implications: 'Wearables: New Interactions and New Opportunities'"

"IT Strategists Must Prepare for the Rise of Virtual Personal Assistants in the Workplace"

"Developing Your SaaS Governance Framework"

GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp