

WINDWARD ROCK RESEARCH

WORLDWIDE IT

FEBRUARY 2017

FROST AND SULLIVAN • FORRESTER • GARTNER • ABI •
IDC • 451 RESEARCH • HARVARD BUSINESS REVIEW • LAWFARE

To Lead a Digital Transformation, CEOs Must Prioritize

According to Harvard Business Review writer Laurent-Pierre Baculard, Partner Bain & Company given the pace at which digital innovation is disrupting industries globally, it's not surprising that most CEOs feel pressure to find and deploy the right technology as fast as their budgets will allow. Many are discovering, however, that becoming a digital leader isn't simply a matter of technological savvy. It's about creating an agile organization that can detect what type of change is essential and respond quickly with the most competitive solution.

In our experience, most companies are already steeped in technology and learning fast about how it can transform their businesses. Typically, teams in the field are well aware of the digital threats and opportunities within their area of the organization – usually more so than the corporate center. They have launched their own apps, deployed robotics, established partnerships with digital players, or are using data to analyze their business and make better decisions.

To do that effectively, CEOs need a holistic view of the digital threats and opportunities facing key parts of the business, and a way to link them to an overall vision for how digital is reshaping the competitive landscape. Three ways to manage the digital transition are:

Define where change is needed most: Digital technology affects every company differently, but it tends to create or destroy value in four critical areas of the organization: customer engagement,

**WINDWARD ROCK RESEARCH
WORLDWIDE IT**

Choreograph the change: Even the clearest digital strategy will fail if your people are unprepared to embrace it. As critical as defining where you need change is setting up the capabilities and processes that will enable it. IT, for instance, is very often the tightest digital choke point because it is mired in old processes and needs significant reshaping to link it more closely to strategy, while creating a more agile approach to development. It is also essential to develop key capabilities in data analytics to make better decisions using the flood of new information flowing through the organization.

possible solutions across silos, wading through validation loops and meeting threshold tests simply isn't fast enough.

Empower people: One clear implication of this approach is the central importance of an orchestration model for digital —prototyping, risk-taking, and mobilizing the frontline to push concrete initiatives.

Only the CEO can manage this process by breaking down the appropriate boundaries, giving teams permission to set new rules, and providing the strategic framework to buttress the new order. It often

New IDC Survey Finds Widespread Privacy Concerns Among U.S. Consumers

A recent survey conducted by International Data Corporation (IDC) finds that a whopping 84% of U.S. consumers expressed concern regarding the security of their personally identifiable information (PII) and 70% told IDC that their concern is greater today than just a few years ago. The newly published special study, which measures consumer privacy sentiment across four vertical industries (Financial Services, Healthcare, Retail, and Government), also includes the following key findings:

- **Demographics Matter:** Younger consumers, those age 18-35, demonstrate a higher concern for their personally identifiable information than do their 36-50 year-old counterparts.
- **Call to Action:** Hyper awareness and growing sensitivity toward data exposure appear to have consumers on the verge of making serious changes in their behavior.

Gartner Says More Than 40 Percent of Data Science Tasks Will Be Automated by 2020

More than 40 percent of data science tasks will be automated by 2020, resulting in increased productivity and broader usage of data and analytics by citizen data scientists, according to Gartner, Inc. Gartner defines a citizen data scientist as a person who creates or generates models that use advanced diagnostic analytics or predictive and prescriptive capabilities, but whose primary job function is outside the field of statistics and analytics.

With data science continuing to emerge as a powerful differentiator across industries, almost every data and analytics software platform vendor is now focused on making simplification a top goal through the automation of various tasks, such as data integration and model building.

Gartner also predicts that **citizen data scientists will surpass data scientists in the amount of advanced analysis produced by 2019**. A vast amount of analysis produced by citizen data scientists will feed and impact the business, creating a more pervasive analytics-driven environment, while at the same time supporting the data scientists who can shift their focus onto more complex analysis.

Machine Learning in Cybersecurity to Boost Big Data, Intelligence, and Analytics Spending to \$96 Billion by 2021

Cyber threats are an ever-present danger to global economies and are projected to surpass the trillion dollar mark in damages within the next year. As a result, the cybersecurity industry is investing heavily in machine learning in hopes of providing a more dynamic deterrent. ABI Research forecasts machine learning in cybersecurity will boost big data, intelligence, and analytics spending to \$96 billion by 2021.

ABI Research finds the government and defense, banking, and technology market sectors to be the primary drivers and adopters of machine learning technologies. User and Entity Behavioral Analytics

Increased Ransomware and Targeted Attacks Generate Double-digit Growth Opportunities for Asia-Pacific Network-based Advanced Malware Analysis Solutions

In the Asia-Pacific region, network-based advanced malware analysis solutions (NAMA) are in high demand due to a rise in advanced malware, ransomware, state-sponsored and cyber-attacks on government agencies, bank systems and critical infrastructures. Organisations and governments are seeking effective, real-time advanced detection technologies and security solutions to prevent potential security breaches, liabilities, and financial and reputation losses.

“Local managed security providers must build partnerships with NAMA solution vendors to drive growth and adoption for enterprises in Asia-Pacific,” noted Tien. “Networking appliance manufacturers can form original equipment manufacturer partnerships with cloud-based NAMA providers to bring advanced protection against malware attacks in the network and drive adoption of NAMA technologies.”

Application containers will be a \$2.7bn market by 2020

The application container market will grow from \$762m in 2016 to \$2.7bn by 2020, according to 451 Research's latest Cloud-Enabling Technologies Market Monitor report. Despite making up a relatively small portion of the overall Cloud-Enabling Technologies (CET) market, application containers will see the fastest growth compared to other segments, with an estimated CAGR of 40% through 2020.

One of the most remarkable things about the emergent application container ecosystem and market is the number of vendors large and small that are meaningfully leveraging or offering application-container technology and support. 451 Research has identified and currently tracks 125 application container vendors – and expects new market entrants to emerge quarterly, including many yet to be identified as container providers.

“Current estimates are conservative,” said Jay Lyman, Principal Analyst, Cloud Management and Containers at 451 Research. “In the three years we’ve been tracking the OpenStack market, we’ve watched it grow from just 30 vendors in 2013 to more than 91 vendors today. We will be tracking the container market closely to see whether that translates into even higher revenue and faster growth than with OpenStack.”

**WINDWARD ROCK RESEARCH
WORLDWIDE IT**

**Forrester CEO George Colony's Blog:
The Counterintuitive CEO – an Existential Threat**

A message for CEOs: You are slowly going out of business, and many of you don't know it yet.

Your customers demand reliable and compelling experience, enabled by your business technology (BT). If that technology fails, or if you fail to provide that technology, you will lose customers and market share. Your company will be acquired, broken up, or stagger into oblivion as an irrelevant zombie.

Early evidence? Store closings at Wal-Mart and Macy's are exhibit A, but stress fractures are appearing in financial services (Bank of America), telecommunications (Comcast), and the travel industry (United). Now none of these companies are going to disappear in the near term. But the pressure and time of "Customer geology" spell long-term trouble.

Worldwide Spending on Robotics Will Reach \$188 Billion in 2020 Fueled by New Use Cases and Expanding Market Acceptance, According to IDC

Worldwide spending on robotics and related services will more than double by 2020, growing from \$91.5 billion in 2016 to more than \$188 billion in 2020, according to the newly updated *Worldwide Commercial Robotics Spending Guide* from International Data Corporation (IDC).

"The market for robotics continues to experience tremendous growth," said John Santagate, research manager, Supply Chain at IDC Manufacturing Insights. "This growth is really fueled by a combination of technology improvements, expanded use cases, and acceptance in the market. Innovators in the field of robotics are delivering robots that can be used to perform a broader range of tasks, which is helping to drive the adoption of robotics into a wider base of industries."

growth of robotics adoption in general industry roles, and some of the leading suppliers we tracked have enjoyed compound annual growth rates of more than double that for automotive industry for the past few years."

On a geographic basis, the Asia/Pacific region, including Japan, will account for more than two thirds of total robotics spending throughout the forecast. Europe, the Middle East, and Africa (EMEA) is the

second largest region with expenditures of \$14.7 billion in 2016, followed by the Americas with a 2016

Gartner Survey Finds That Most Smartphone Users Spend Nothing on Apps

Over half of smartphone users spend no money on smartphone apps (paid-for downloads and in-app transactions), according to a new survey by Gartner, Inc. However, end-user spending on in-app transactions continues to rise.

"Where users are prepared to pay for apps, spending on in-app transactions is on the rise — up 26 percent from 2015 — while spending on paid-for downloads only increased 4 percent in 2016," said

Age and gender also influence spending levels. Older millennials (people aged 25 to 34 years) are the biggest spenders on both paid-for downloads and in-app transactions, with their in-app transactions

other name for the in-app transaction business model) that lets them try an app before deciding whether to spend money on it.

"Consumers' increased preference for in-app transactions is a clear sign that technology product marketing leaders working for app providers should invest in this model to provide flexibility in how they engage with app users," said Ms. Baghdassarian.

ABI Research Unveils its NRF 2018 Market Predictions, One Year Early

With NRF 2017 just days away, retailers can expect a continuation of 2016 technology trends like mPOS, staff handhelds/wearables, camera analytics, and interactive mirrors with AI, chatbots, IoT and VR replacing omnichannel as this year's overused and oversold buzzwords. But smart retail is in a state

In its latest report, Smart Retail: Predictions for 2018, ABI Research identifies a number of key trends that will shape in-store retail IoT:

- Dynamic pricing technologies
- 3D sensing
- Handset-based SLAM technologies
- Attribution/retargeting
- Next-generation labels and signage

performance, and drive new revenue. This is an essential first step in facilitating the move to retail IoT.

“A retailer can deploy an IoT platform with the latest in artificial intelligence, but if the wrong I/O edge technologies are in place, the system falls down,” concludes Connolly. “The Amazon Go concept is a great example of this, combining a variety of edge technologies in-store to significantly streamline the shopping process and build a service that will excite its customers.”

Learning Management Systems and Lecture Capture Solutions: Employee Engagement Drives New Growth Opportunities

Tremendous technological innovation, solid movement to the **cloud**, and user-centric product development strategies characterize today's global enterprise learning management systems (LMS) and lecture capture solutions (LCS) markets. These advances are fueled mainly by stringent compliance requirements in **high-risk industries**, where employee learning is mission-critical to organisational success. Employers are also utilizing LMS to deliver training that helps employees fill skill gaps and advance their careers, thereby building employee loyalty and reducing attrition.

“Global changes in workforce demographics, employee expectations, and how and where work takes place are compelling enterprises to deploy LMS and LCS to manage and deliver employee **training anytime and anywhere**, identify and bridge skill gaps, and support **career mobility**,” said Digital Transformation Industry Analyst Deviki Gupta.

The **main challenges** for the markets are:

- The vast majority of small and medium businesses remain **unaware** of various viable learning options for training their employees or lack **funds to invest** in training solutions despite having formal eLearning policies.
- The **high costs** of LMS and LCS often induce clients to choose piecemeal, rather than company-wide, deployment in order to make initial investment more manageable.

“In such a market, vendors who are on top of **innovation**, provide an exceptional user experience, keep up with compliance requirements, and have well-trained **customer support** will be in high demand,” said Gupta.

**Forrester's Enza Iannopolo's Blog – Not Only GDPR.
A New Set Of Privacy Rules Is Here.**

Just after a few months since the European Parliament approved the final version of the new General Data Protection Regulation (GDPR), the European Commission is working on updating yet another set of privacy rules. The European Commission published a new text that, when approved, will replace the current ePrivacy Directive: the EU law that ensures confidentiality of communication and the protection of personal data in the electronic communications sector.

While the Commission plans to complete the reform process quickly enough to allow the new law to come into force in May 2018 together with the GDPR, the road ahead is long and tortuous. In fact, both the EU Councils of Ministers and the EU Parliament must agree and approve the final text.

While EU policy makers aspire to finalize a new version of the ePrivacy Directive that goes hand-in-hand with the GDPR, it's a task for all companies to update their processes, technology, workforce's expertise, and oversight mechanisms to comply with both sets of rules. To meet compliance requirements consistently and without redundancies, it's crucial that firms understand what's changing and how ahead of time. According to the proposed text, the new ePrivacy law will:

1. **Be a regulation.** As the GDPR, the updated version of the ePrivacy Directive will be a regulation. This means that one single law will apply to all countries of the European Union.
2. **Have fines up to 4%.** In line with the GDPR, also the new regulation will include fine up to €20 million, or 4% of companies' annual global turnover, whichever is the highest.
3. **Reach companies beyond telcos.** The new rules will apply not only to traditional telcos, but also to providers of electronic communications services, including internet access, instant messaging applications, e-mail, internet phone calls, and personal messaging provided through social media.

6. **Call for transparent notices when tracking customers' physical activities.** Firms that scan their customers' physical devices to know, for example, how many people are in a queue or whether a new customer is entering their shop, must inform customers about this activity to include information on how the customer can take control over the tracking, including opting out of it.
7. **Give new rights to users.** The law also allows for potential compensation of users that suffered material or no-material damage as a result of the infringement of the rules.

**The Truth About Blockchain – written by Harvard Business Review's
Marco Iansiti; (David Sarnoff Professor of Business Administration)**

Contracts, transactions, and the records of them are among the defining structures in our economic, legal, and political systems. They protect assets and set organizational boundaries. They establish and verify identities and chronicle events. They govern interactions among nations, organizations, communities, and individuals. They guide managerial and social action. And yet these critical tools and the bureaucracies formed to manage them have not kept up with the economy's digital transformation. They're like a rush-hour gridlock trapping a Formula 1 race car. In a digital world, the way we regulate and maintain administrative control has to change.

Blockchain promises to solve this problem. Blockchain is an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way. The ledger itself can also be programmed to trigger transactions automatically.

True blockchain-led transformation of business and government, we believe, is still many years away. That's because blockchain is not a "disruptive" technology, which can attack a traditional business model with a lower-cost solution and overtake incumbent firms quickly. Blockchain is a *foundational* technology: It has the potential to create new foundations for our economic and social systems. But while the impact will be enormous, it will take decades for blockchain to seep into our economic and social infrastructure. The process of adoption will be gradual and steady, not sudden, as waves of technological and institutional change gain momentum.

No matter what the context, there's a strong possibility that blockchain will affect your business. The very big question is when.

**EMEA Cloud IT Infrastructure Revenue Grows 19.5% to \$1.5 Billion in 3Q16,
According to IDC**

According to the International Data Corporation (IDC) WW Quarterly Cloud Infrastructure Tracker, IT infrastructure spending (server, disk storage, and Ethernet switch) for public and private cloud in Europe, the Middle East, and Africa (EMEA) grew 19.5% year on year to reach \$1.5 billion in revenue in the third quarter of 2016.

"IDC expects this market to reach a value of \$10.9 billion by 2020, from the five-year forecast, or 35.4% of the total market expenditure. Fueled by increasing maturity and adoption rates of many new cloud-dependent technologies such as the Internet of Things, cloud continues to represent an area of tremendous growth for the European infrastructure sector," said Kamil Gregor, research analyst, European Infrastructure Group, IDC.

Regional Highlight

"In Western Europe, we are beginning to see not only specific solutions based on 3rd Platform and Innovation Accelerator technologies, but increasingly often innovative solutions that combine multiple technologies to harness unique value that none of the technologies could unlock alone," said Gregor. "For example, several emerging industry clouds in the region combine data from the Internet of Things edge devices with real-time and Big Data analytics in subverticals such as advanced building automation, manufacturing asset management, and predictive maintenance.

"Regulatory compliance is becoming an increasingly important inhibitor of cloud adoption in the region, mainly due to political volatility in the EU, both in 2016 and potentially continuing throughout 2017, and as we approach the end of a two-year transition period for the EU's General Data Protection Regulation. Enterprises at the bleeding edge of innovation are looking into ways of mitigating these issues, for example by taking blockchain technology from the world of financial transactions and applying it to automation of policy compliance in complex cloud environments."

**IoT Managed Security Services to See Significant Financial Impact
from Industrial Applications**

Industrial applications are set to be the core focus for IoT Managed Security Service Providers (MSSPs) with ABI Research forecasting overall market revenues to increase fivefold and top \$11 billion in 2021. Though OEM and aftermarket telematics, fleet management, and video surveillance use cases primarily drive today's IoT MSSP service revenues, continued innovation in industrial applications that include the connected car, smart cities, and utilities will be the future forces that IoT MSSPs need to target.

"Security adoption will thrive across the industrial segment as manufacturers seek to enable new levels of efficiencies, while ensuring that they are not only providing continuous operation, but also supporting applications critical to health, safety, and life," says Phil Sealy, Senior Analyst at ABI Research. "In addition, secure Over the Air, or OTA, applications present a new and significant revenue opportunity for IoT MSSPs to offer digital upselling and upgrade opportunities."

“Although the monetization opportunity may not yet be well understood within the consumer segment, the ability to add new features across the life cycle of a device should not be underestimated,” concludes Sealy. “Security will, in the future, form part of the purchase choice, directly driven by improved security education and a broader demand to protect digital assets in the same sense as users protect their physical assets today. For this reason, security service providers, although largely invisible today, may become the household names of tomorrow as IoT security moves from a requirement to a product differentiator.”

Nanotechnology to Increase Cost Efficiency by Streamlining Global Medical Devices Value Chain

Nanotechnology-based **medical devices** reduce costs across supply and demand value chains, as they firmly place the bargaining power in the hands of large medical device manufacturing companies. By incorporating nanotechnology into their products, original equipment manufacturers (OEMs) can

“Owing to the significant commercialization potential of nano-materials, large medical device companies have partnered with university spin-offs and research institutes to co-create solutions that improve the effectiveness of therapies,” said Frost & Sullivan TechVision Industry Analyst **Arjunvasan Ambigapathy**. “Researchers particularly focus on developing products for high-growth medical device sectors such as wearables, point-of-care diagnostics, advanced wound care, and drug delivery systems, targeting conditions other than cancer.”

There are few impediments to the rapid commercialization and adoption of nanotechnology during development of medical devices. Even the challenges inherent in the scaling up of nanocoating technologies and nano-functionalization of surfaces for the improved performance of devices are almost negligible.

**WINDWARD ROCK RESEARCH
WORLDWIDE IT**

**Analyze This! Cisco Spends \$3.7B To Buy AppDynamics
reports Forrester's Milan Hanson**

Cisco's intent to acquire AppDynamics is quite a surprise. Then again, it isn't. **It's a surprise** because AppDynamics was one day away from its IPO, giving nary a hint of courting a suitor. That would be an awfully expensive and troublesome camouflage. And if it was camo, it was amazingly airtight in this notoriously leaky information age.

It's a surprise because AppDynamics was one day away from its IPO, giving nary a hint of courting a suitor. That would be an awfully expensive and troublesome camouflage. And if it was camo, it was amazingly airtight in this notoriously leaky information age.

It's not a surprise because AppDynamics' APM competitors have been rapidly broadening their monitoring to yield better analytics with fewer blind spots. Cisco gives AppDynamics an exceptionally clear view of network performance and AppDynamics gives Cisco a clear view of application performance. APM solutions must continue to expand their data ingestion to provide optimum value.

There's really only one contentious point, and that's analytics. Cisco will have to position its Tetration analytics engine viably with AppDynamics' "App iQ" analytics platform. Longer-term, Cisco will need to show integration that reduces work for infrastructure & operations staff and delivers value throughout the enterprise.

**Lawfare's Charley Snyder and Michael Sulmeyer
Assess the Draft Cyber Executive Order**

Amidst the whirlwind of executive orders and presidential memoranda that have been in the news, it was easy to miss a purported draft of President Trump's first executive order (EO) covering cybersecurity issues, leaked to the *Washington Post* and released on Friday, January 27. The order, titled "Strengthening U.S. Cyber Security and Capabilities," calls for several 60- and 100-day assessments of the state of U.S. cybersecurity and the identification of areas of improvement.

WINDWARD ROCK RESEARCH WORLDWIDE IT

At its core, this order loosely follows a traditional formula to estimate risk: assess the threat from adversaries, your vulnerability to that threat, and the consequences if the vulnerability is exploited. In essence, the Administration wants to get a better idea of our nation's vulnerabilities and the threats it faces and to determine what tools we might have at our disposal to protect critical infrastructure from those adversaries.

Policy and Findings — The policy and findings sections reaffirm several of the touchstones we have come to expect from the federal government: the need to preserve the Internet as engine of prosperity and innovation without jeopardizing our privacy or allowing criminals free reign; the dynamic nature of the domain and the increasingly interdependent nature of information technologies and critical infrastructure; and the vulnerabilities found in both private and public sector networks. Information security and cyber issues pose a formidable challenge for federal government agencies whose authorities often predate computing and networking by decades.

Policy coordination — This section indicates that the management of cyber issues will be consistent with the newly-signed National Security Presidential Memorandum (NSPM) 2, which establishes the National Security Council organization and coordination. This, and the elevated stature of the Homeland Security Advisor as on par with the National Security Advisor, likely will mean an elevated level of attention on these issues for this administration.

Review of Cyber Vulnerabilities — The first substantive section of this executive order is about vulnerabilities. As one of our colleagues, Ben Buchanan, likes to say: in the United States, we may have some very nice cyber rocks, but we live in a very glassy house.

One factor bears mentioning. Any Chief Information Security Officer worth his or her salt knows that before diving into vulnerabilities, it is important to get a firm grasp on what assets are most worth protecting. Just because a network is most vulnerable does not mean that it is most worth spending your next dollar to protect.

Review of Cyber Adversaries — The order then tasks the Director of National Intelligence (DNI) to deliver to the President what is, in essence, a National Intelligence Estimate of the identities, capabilities, intentions, and vulnerabilities of our top adversaries in cyberspace. This is the kind of product that the Intelligence Community likely would prepare for a new administration in any case. Given the present tension over and politicization of the activities of one of the primary threats to U.S. networks—Russia—it is interesting that the review will not be strictly conducted by the Intelligence

What's Missing?—Though we can't fault the administration for choosing certain areas to prioritize in its first few months, there are a few additional areas the administration will need to turn its attention to if it wants a truly comprehensive review of cybersecurity issues:

- This draft of the EO neglects to mention anything about international cooperation in cyberspace and the State Department's multi-year effort to build consensus around norms of behavior.
- We already noted the conspicuous absence of the FBI; likewise, consideration of broader criminal and legal issues is missing from the order. At some point, the Trump administration will need to address law enforcement's access to data particularly encryption.

**Internet of Things Spending Forecast to Grow 17.9% in 2016 Led by
Manufacturing, Transportation, and Utilities Investments,
According to New IDC Spending Guide**

Worldwide spending on the Internet of Things (IoT) is forecast to reach \$737 billion in 2016 as organizations invest in the hardware, software, services, and connectivity that enable the IoT. According to a new update to the International Data Corporation (IDC) *Worldwide Semiannual Internet of Things Spending Guide*, global IoT spending will experience a compound annual growth rate (CAGR) of 15.6% over the 2015-2020 forecast period, reaching \$1.29 trillion in 2020.

**Surging Wi-Fi Traffic and New IoT Applications to Spike Wireless IC Shipments
by 54% by 2020**

Surging Wi-Fi traffic, new uses cases, and emerging IoT applications will result in a nearly 54% increase in wireless IC shipments by 2020, forecasts ABI Research. The short-range wireless connectivity market technologies—including ZigBee, Thread, Bluetooth Low Energy (BLE), Z-Wave, Wi-Fi, and NFC—will continue to evolve to meet new market demands, as evident with various new and upcoming enhancements. These include Bluetooth 5 and Bluetooth Mesh, the ZigBee Alliance’s reveal of dotdot language for the IoT, W-iFi HaLow (802.11ah), WiGig (802.11ad), new Z-Wave security enhancements, and the growth of ICs that combine several of these connectivity solutions.

Wi-Fi’s continued evolution will come in the form of several new protocols. 802.11ax will focus on overall network efficiency improvements rather than simply boosting peak speeds. 60GHz WiGig (802.11ad) will improve Wi-Fi’s suitability for 4K streaming, docking, and VR applications. The sub-1GHz HaLow standard (802.11ah) will open up new opportunities in low-power and in an extended range of IoT applications.

Wi-Fi chipsets that incorporate 802.11ax, WiGig, or HaLow technologies will make up 60% of all wireless IC shipments by 2021. However, both WiGig and HaLow represent a new direction for Wi-Fi and will face unique challenges in terms of creating a new ecosystem in different bands.

Lastly, Z-Wave’s strong interoperability will remain a major advantage and key value proposition, allowing service providers and others to provide a manageable and more advanced smart home solution that can resonate beyond early adopters and reach a mainstream audience. Further security enhancements through the new S2 security framework and strong backing from key home security vendors will help the technology grow in the years to come.