Executive Report

TRENDS, FORECASTS AND ANALYSIS FOR EXECUTIVES IN THE IT INDUSTRY AND IT ORGANIZATIONS

27 febuary, 2018

VOLUME 31

Marketing is marketing and marketing is a business-case …

Marketing is marketing right? There's marketing that works, and there's marketing that doesn't work, (obviously). In most cases, marketing to private persons tend to speak directly to the unconscious of the persons mind, neuromarketing if your fancy-schmancy. On the other hand, when marketing is directed to (for the sake of the example) towards the same person but during work-hours, when the person is "business-person" the marketing is based on cold facts and measurable business-values. Why is that?

- Are your decisions in some way colored by your own perception rather than absolute facts and the optimal business value?
- Have you ever hired or done business with someone just because they seem trustworthy from a `judged by my heart´ kind of way?
- Do you prefer a glass of alcohol on friday evening, or do you rather sip on a cup of lubricant or motor-oil?

You get the point … You're not supposed to follow your heart when at the office, that's a luxury you only get to try at home, and be a robot at work …

Wrong … If you were to measure your private life, would it be a successful endeavor in the long run? Probably… Family, bank funds pointing right up, husband turning towards admitting to being feminist … or a wife that gives your whisky-collection thumbs up as long as it doesn't take up too much space, no matter monetary investment. Following your heart has taken you quite a long way, hasn't it?

So, you're obviously the same person with the same mindset whether you're in your grey suit, or in your Metallica shirt at home, with the same decision-making presets when it comes to making choices. With that said, you should put a little more heart into your decisions. Also, you got a lot of experience from IT and management, so your gut/heart is probably more reliable than the general term "listen to your heart/gut" …

Your heart gives you ROI within a couple of weeks, while budget numbers are measured through quarters, but probably year basis. If things don't get measured, they can't be managed. Your heart gives you the best base for measures there are, use it!

Johan Lennström
Editor in Chief, Executive Report
johan.lennstrom@executivereport.se
070-615 06 98

Bcs

The practical applicability of AI

Machine learning and cognitive computing are on track to become some of the most widely applicable technological movements we have ever seen. Together, they are set to be primary drivers of the fourth industrial revolution and will cause social revolution on a global scale.

Individuals and organizations must begin preparing for this eventuality. During the digital revolution, those who were slow to adopt, or those who eschewed the internet, suffered severely because of their indecisiveness. Since then, lessons have been learnt, and, more than ever before, society has become aware of the effect of technological change. We can easily see this technological revolution unfolding around us, and its advances are likely to occur at a surprising rate.

Now is the time to educate, to consider how the applications of AI impact business, to experiment, and to understand how AI should be effectively progressed into production.

This does not mean retraining to become a data scientist. But at the very least, organizations should learn about the practical applicability of AI. This is especially important for business leaders, many of whom don't have the appropriate knowledge to effectively identify applicability to their business. More importantly, this knowledge provides leaders with visibility into how technology advances will change their operating market, as well as the impact their employers, clients and competitors.

Organizations that fail to understand the impact of AI - regardless of industry sector - risk going out of business.

Experimentation should be a fail fast, no regrets undertaking, fed by hypotheses from across the business. While machine learning often requires a significant amount of data, leaders should not delay experimentation because their data is unclean and fragmented. Instead, an experimentation capability that is empowered to obtain data from across the business should be formed.

This capability should be able to utilize the tools they feel most comfortable with, enabling them to try new technologies and approaches. The major public cloud platforms offer an excellent environment for this with ephemeral compute and tools like Azure ML Workbench and AWS SageMaker, alongside a raft of excellent pay-per-use APIs. These tools have also been designed with the data science process in mind, building in the ability to promote production more simply.

Opportunities should be created for development and experimentation teams to work together. This exposes engineers to the data science process and data scientists to engineering rigour - an area of common complaint when progressing to phases beyond experimentation.

Those already experimenting with AI are discovering a vast range of potentially valuable applications. Unfortunately, in many cases, their ability to prove these out in production is limited by enforced dependency on slow-moving enterprise-wide initiatives; data and cloud strategy and data lake programs, for example.

Businesses should be cautious when undertaking such initiatives, particularly when it comes to the manner of their implementation and enforcement. The same can be said of poorly delivered cloud strategies that are simply 'worked around', thereby increasing security risk, among other issues. Removing these dependencies until the appropriate point is key to demonstrating the value of AI in production environments.

The progress of AI and its effect on society is exciting, but a measured approach is required. While many forward-looking organizations are already experimenting with AI, it is crucial that they do not create a backlog of successful experiments that cannot progress. They can achieve this by expanding their views and modifying their approach beyond experimentation. Those organizations which succeed in doing so will benefit greatly at the expense of those who do not. ●

#AI #MachineLearning #Innovation

Harvard business review

How cloud is changing management

History suggests that the main way information technology changes management is through changes in how information is gathered: the large-scale analysis of Operations Research reflected painstaking data collection around a few metrics, which were transferred to punch cards. BPM reflected the interactions of different stakeholders, from product creation through supply chain to final assembly.

Theories and practices of management often spring from the opportunities created by new technologies. Interchangeable parts spurred ideas about structuring assembly lines and logistics. The complex calculations of the field known as Operations Research were enabled by mainframe computing. Client-server technology begat enterprise resource planning systems, and the consequent system-wide visibility that was required for what we call business process management (BPM).

That makes it imperative to start thinking about how management will be changed by the most impactful information technology of our time: cloud computing. What does it allow us to do differently, and how will that change the way we do things in the future?

How organizations are changing

With cloud, information travels rapidly in both directions, across computing systems that, with attributes like virtualization, scaling up or down to handle bigger workloads, or automated security patching across thousands of machines, are far more flexible. This will likely mean a more flexible work structure as well, in the interest of products and services that ideally can be adjusted to anticipate customer needs. Key to the new system are rapid data collection and analysis, followed by over the air changes to product software.

Likely outcomes of the move to cloud include changing how products are designed; closer collaboration between the corporate IT department and other business units, including sales, finance and forecasting; and more customer interaction, even to a point of jointly developing products with their consumers. In particular, new ways of writing and deploying software will encourage new types of faster-acting organizational designs. And the best way to anticipate how these changes will occur is to hear from companies already aggressively implementing them.

It's already changing organizations, by moving IT from a cost center to something with a place at the table in a lot of different meetings. Public cloud computing, offered by companies like Amazon Web Services, Microsoft Azure, Google Cloud, is still viewed by many as a cheaper and more efficient way for companies to store and process data. The cost may be lower, but like traditional computers, it is still a cost.

Lower costs have been reason enough for many companies to shut down their proprietary data centers and consume computational power and attendant software as a series of on-demand services. Others use cloud computing software in their own data centers, as a means of increasing resources and working faster.

How it effects product design and customer experience

As cloud technology improves, however, it is becoming easier for companies to create products and services within the cloud, or model new products or marketing campaigns as cloud-based software prototypes. The cloud is also a common repository for the collection and analysis of new data, and the place where an increasing number of AI-operations, like image and speech recognition, are conducted.

The evidence is already there, as startups increasingly conceive of their goods and services largely as software-centric entities, from which data is continually derived. Changes and upgrades become part of a continuous process. Organizational functions blur as processes become increasingly iterative.

The ride-hailing company Uber has stressed the importance of its hybrid cloud model to ensure not just constant uptime, but an indivisible relationship between product development and deployment. Uber is able to model a virtual fleet of taxis from private cars through a combination of mobile software, large-scale data analysis, mapping, and social networking.

What else needs to change?

The constant relationship between management theory and applied technology shouldn't be too surprising. William Hewlett, a founding father of Silicon Valley, famously said "you cannot manage what you cannot measure." It seems to logically follow that opposite also holds true — what and how you measure something influences the way it is managed. How soon will cloud be as influential for management as the mainframe or client-server computing? Major technology improvements may lag productivity gains for years, even decades. The most tantalizing reason why: An ecosystem of other changes has to arise, along with new thinking about how the technology should be used, in order for it to have full impact.

Software-based advances like AI and cloud-style software will find a place faster than many of the earlier advances. For one thing, lower costs mean they can be quickly adopted by startups unencumbered by legacy costs and practices. And, unlike hardware-based advances, the influence this time will be from software — in particular, what happens when teams throughout the corporation build products and services using what is termed cloud-native software. With the cloud, processes can be replicated quicker. But you still need three things to be updated before you fully take advantage: Organizational innovation, trained human capital, and social institutions, like infrastructure and regulation, that accommodate new technologies.

The shift to "cloud native" organizations

The way software is conceived of for cloud computing may turn out to be as important as the physical infrastructure of cloud (which is millions of computer servers dispersed around the globe, connected by high speed fiber optic lines.) "Cloud native" software approaches stresses ease of use and low-impact alteration of components of any given software application. Massive applications are subdivided into a series of "microservices" that can be tweaked with little effect on a running piece of software.

Traditional complex software often has a series of relationships, called dependencies, with other lines of code, requiring big rewrites for even trivial changes. Think of it as the way a plant's roots can grow over a big area, and intermingle with other roots. By orchestrating microservices into highly portable units, called containers, the dependencies are potted.

That means it is possible to deploy and manage an application globally, from a single location, with relatively little hassle. Kubernetes, the most popular open source software for orchestrating such container usage, was originally developed inside Google to run the company's many global applications, and easily alter products and issue software fixes at the greatest possible scale.

Google now runs about 2 billion containers a week on its in-house version of Kubernetes. The new way of deploying software, also gives you visibility on where and how it is consumed, providing information about future costs. That modifies the job from solely capital expenditure to operating expense, and effectively a collaborator on growth. In 1967, still early days in the Information Technology revolution, John Culkin had a brilliant insight. "We become what we behold," he wrote. "We shape our tools and then our tools shape us." Five decades on, we have the benefit of much IT history, and can think how we, and our organizations may be shaped by new technology. As our systems and people gain in their capabilities to adapt to changing markets, every aspect of a business will become more responsive.

Fixed job roles, like software engineering or financial planning, may evolve towards domain knowledge, which is shared in collaborative teams, brought together and disassembled for some part of a product lifecycle. Companies may partner more deeply, taking advantage of each other's comparative advantage to meet a new market need. Managers will need to concentrate more than ever on skills such as collaboration, empathy, learning, and novel rewards to create an organization more adaptive than the cloud computing IT tool it beholds. ●

#OpenSource #Cloud #CIO #CEO #Management #OrganizationalStructure

Gartner

Why DevOps is a game-changer for security

DevOps represents a kind of cultural revolution in which the creation and deployment of software and services happen at an extremely accelerated pace. That said, this process has largely taken place outside the purview of information security (InfoSec) and often without its knowledge or involvement.

As a result, security teams have struggled to keep pace or, even more seriously, have not been engaged at all. Even when they are engaged, security teams tend to slow the overall development process with their own linear approaches and mindsets.

Yet DevOps presents InfoSec with the perfect opportunity to move from a reactionary response to one where safeguards, proactive testing, and prevention are automatically integrated throughout the development lifecycle.

Built-in security

The practice of integrating security into DevOps is quickly gaining momentum. By 2021, secure DevOps processes will be embedded in 80% of rapid development teams, up from 15% in 2017.

In response, InfoSec teams should shift from a reactive approach to one that incorporates built-in security controls throughout the development process. With integrated security tools in place, developers never have to leave their continuous deployment toolchain environment. Moreover, organizations are eliminating the risk that developers will simply choose to bypass separate security tools. Built-in security ensures the quality and integrity of products and software that are constantly evolving, and it reduces operational costs by fixing defects early in the software development lifecycle. Built-in security testing enables developers to move fast, confident that mistakes and vulnerabilities will be resolved before deployment. By collaborating, and integrating security at multiple points in DevOps workflows, InfoSec teams can assess integrity with each new iteration, and leave behind labor-intensive manual testing.

Automation

Many organizations with strong DevOps processes generate dozens – sometimes hundreds – of iterations a day of software and services. Moreover, developers constantly run QA tests during builds covering unit, API, and integration testing to improve code quality. In these fast environments, manual testing and the linear model for security are simply inadequate. For example, traditional one-time gating and penetration testing delays deployments, and decelerates high-velocity development cycles.

Automation compensates by ensuring that high levels of security exist across all areas of DevOps, not only as a seamless part of a developer's integrated development environment (IDE), but also within the continuous integration and continuous development (CI/CD) toolchain. For example, security testing can become another quality control that's incorporated into QA. Automation guarantees that application security is an inherent part of the build process and facilitated by DevOps itself as software evolves.

When you consider the limitations of outdated processes like gated checks, or the alternative of no security at all, then it's clear why automated security is crucial to the DevOps process.

Proactive prevention

In general, InfoSec teams spend inordinate amounts of time identifying and remediating security vulnerabilities.

The process of applying security protections in the final stages of development, or patching vulnerabilities after deployment, are both time-consuming and resource intensive. This challenge is often compounded by the tedious process of identifying individual application and asset owners – especially in the case of micro-services, which frequently involves many owners.

By integrating InfoSec early in the DevOps process, many vulnerabilities can be prevented, and cybersecurity teams can ensure that defects cannot be exploited in production. Taking such an approach reduces operational costs by proactively addressing security rather than responding on a case-by-case basis and putting out fires.

Moreover, being proactive can also negate time-consuming and costly incident response efforts. Finally, preventing potential vulnerabilities enables InfoSec leaders to implement higher-value programs that more effectively support compliance, and improve risk management.

Putting reasons in action: securing application containers

DevOps teams are rapidly adopting containers to enable the continuous development of new applications and services. In fact, containers are one of the hottest innovations in enterprise IT, with 40% annual growth in adoption.

Containers are transformational packages that dramatically accelerate and simplify application development and deployment while lowering operational costs, increasing innovation, and speeding deployments. Standalone, lightweight, and efficient, containers enable seamless portability across different computing environments through write once, run anywhere capabilities.

In addition to greater consistency and more streamlined processes, containers also offer developers increased agility. Yet these extremely short-lived assets can be quite difficult to secure using current vulnerability management techniques. For cybersecurity teams, it requires nearly constant environment scanning with no guarantee of detection. The lack of container IP addresses or logins for credentialed scans further complicates the security process and renders traditional testing ineffective. Finally, remediation or patching is impossible once a container is deployed, requiring a completely new approach to cybersecurity.

A principle means of reaching these new security objectives is leveraging secure DevOps principles. These include moving security testing closer to the beginning of the software lifecycle, adopting automation where possible, and focusing on the actual container image itself.

For example, developers can reduce risks and ensure higher degrees of protection by performing vulnerability and malware checks of container images and certifying compliance at build time. In this secure DevOps model, security tests live in the CI/CD and take less than a minute to complete. These kinds of methodologies are the result of a new IT mindset that emphasizes the primacy of an immutable infrastructure where components are replaced and redeployed rather than changed in place.

Toward that end, adopting a comprehensive container security platform offers an effective means for gaining greater visibility into container images and integrating security into the DevOps pipeline.

A platform approach includes container security solutions that provide the guardrails to keep developers within a certain risk posture, and enforce corporate policy. Having the right platform in place guarantees that developers never have to leave their CI/ CD systems and that every build is protected.

Moreover, a container security platform ensures that testing becomes a fundamental part of DevOps processes without impeding development velocity.

Taking a new approach to organizational security

The increased speed of IT brought on by digital transformation is fundamentally changing how IT security, developers, and corporate end users think and work.

But greater connectivity and faster production can also lead to increased risks. Ensuring effective safeguards requires an organization-wide cultural shift and a new mindset in which cybersecurity becomes the responsibility of all stakeholders. → 9

Tune

Four ways AI is transforming omnichannel marketing

Nearly 40% of marketers say AI, machine learning, or deep learning will be the most transformative technology for marketers in the coming year.

There is little doubt that Big Data married with AI will be the marketing technology story of 2018. That powerful combination will continue to make huge strides in optimizing ad targeting, creative design, and marketing offers where results are measured with hard metrics like clicks and purchases.

Machine learning and artificial intelligence will make the biggest impact on marketing in 2018 – specifically in the retail sector, whose marketing complexities have grown far beyond human capabilities. Humans alone can no longer manage thousands of SKUs, promos, dynamic pricing stockouts, and more, simultaneously.

AI Is making marketing more performance-based

It's one thing to know your target audience based on focus groups, lead scoring, and marketing platforms. It's another to have AI on your side.

AI paired with machine learning can assess not just your customers, but also industries as a whole. AI can scan entire populations and generations of texts, phrases, questions, and shoppers to reveal hidden patterns, solutions, and opportunities in the data. To reap the benefits, create a culture relentlessly focused on performance and measurement, and then use AI to take you even further.

What's key to note is that the technology alone won't lead to success. The brands that leverage AI the best will be those with exceptional digital marketing talent who understand customer needs and who are driven by a performance-focused culture. They will be maniacally focused on metrics to inform where they can optimize customer experiences in real-time.

Through AI, CMOs will have to adapt and evolve their strategies through exposure to new data over time, and play a critical role in business's ability to intelligently transform existing processes without being limited by the speed of humans. The bottom line: It starts with culture. Create one centered around measurement today, and AI will be your competitive advantage in the future.

AI is increasing emphasis on the entire customer journey

A massive 80% of consumers stop using an app within three days. This stat underscore for marketers that it's not just about knowing who leads are before they become customers. It's vital to know how to engage your customers so they stay your customers.

AI can help create a fuller picture of your customers by connecting the dots across their devices and revealing how their needs change with each. AI can also quickly identify patterns among customers to provide insight into the best way to approach them at each stage of the customer journey.

Marketing leaders need to realize that to meet consumer expectations around personalization and real-time, relevant, contextual content, they'll need to turn to AI for help. High performing marketers are already leveraging AI to better understand consumer behavior and make predictions about how customers are likely to interact with their brands, so they can meet each individual customer where they are in their journey.

To ensure you're up to speed, make sure you have technology that can measure across all devices and stages of the customer journey. Ensure you're leveraging AI to deliver the most customized in-app messaging, automated responses, and recommendations.

Acquisition is a start, but engagement and retention are what really matter to the bottom line.

AI is elevating the customer experience

We've all experienced bad marketing: spammy emails, annoying TV commercials, irrelevant banner ads. AI can help with that.

By making marketing more personalized, AI is transforming marketing into something that people truly enjoy. Because AI can sift through massive amounts of customer data and identify patterns with impressive speed and accuracy, it can learn from customers constantly to create more tailored experiences.

AI and machine learning will have the most profound impact on marketing in 2018 because it will fundamentally make marketing more human, which is ironic in and of itself.

This is where a marketer really shines with AI: Use AI to better understand your customers, and then put your creativity to work creating the most compelling marketing possible. For example: In an app, this might mean knowing exactly when a customer loves to hear from you, or which kinds of messages they convert on best. Use that insight to tailor similar messaging for similar customers, and then test those messages with a broader audience, using AI to improve analysis and increase efficiency.

AI is powering customer decisions

The remarkable accuracy AI offers will eventually allow customers to bypass recommendations; they will cut to the chase and trust AI with decisions instead of suggestions. Take travel, for example: A customer could sift through hundreds of hotel recommendations based on filters; or, a customer could trust the recommendation that's best for them based on their past experiences and data from people who like what they like and shop how they shop. As a marketer, consider how you could use AI to make better recommendations for your customers every time they open your app. Given the insight you have into their shopping preferences (both for physical products and variables like time of day, location, and frequency), what processes could you put in place to always surface the right recommendation at the right time? That's where AI not only makes you a better marketer, but also helps surprise and delight your customers. ●

#AI #Machinelearning #ML #Automation #BigData

7→ Consider these recommendations for how you can increase security aware ness and commitment:

DevOps teams

- Embrace security training to understand cyber risks
- Incorporate InfoSec within small, cross-functional teams
- Move security tasks further left in the DevOps toolchain
- Encourage communication across teams and silos
- Designate responsibility for security testing directly to developers
- Ensure that developers never leave their toolchain environment

InfoSec teams

- Perform continuous risk- and trust-based assessments
- Approach application security testing as a continuous improvement process
- Reduce operational risks by breaking down large projects into smaller, simpler changes
- Participate in DevOps scrums and planning cycles
- Embed a security champion model throughout the organization, especially in DevOps
- Prioritize remediation to focus on securing high-level risks, even if that means allowing for low-risk vulnerabilities to persist. ●

#DevOps #OrganizationalStructure #Management #Security

Harvard business review

AI risk should be approached like natural disasters

The risks posed by intelligent devices will soon surpass the magnitude of those associated with natural disasters. Tens of billions of connected sensors are being embedded in everything ranging from industrial robots and safety systems to self-driving cars and refrigerators.

At the same time, the capabilities of AI algorithms are evolving rapidly. Our growing reliance on so many intelligent, connected devices is opening up the possibility of global-scale shutdowns.

The good news is that natural disasters themselves, which caused approximately $330 billion in economic losses globally in 2017, provide a template for how to mitigate the growing and catastrophic risk posed by AI. Like they have for extreme weather and natural disasters, companies can begin to establish international protocols and standards to govern AI not just within their own walls, but also to put in place processes to work with other companies, insurers, and policymakers.

Intelligent device recovery plans

Today, many companies are exposed to intelligent device risks that could harm both their own operations as well as their customers. Yet few have formally quantified the size of their revenue at risk and potential liability. Nor have they set up safety and security protocols for potential Black Swan AI events.

They should. Like the risks associated with natural disasters, companies cannot completely protect against smart-device risks by buying insurance; they must have worst-case scenario recovery plans. Managers have to figure out their higher and lower risk intelligent device vulnerabilities, add in redundant systems, and potentially set up the AI equivalent of tsunami early-warning systems. In addition, they need the ability to switch to manually controlled environments in case AI systems have to be shut down and to recall faulty smart products.

Contingency plans must go beyond a natural disaster playbook. Given the many potential points of connectivity, it will be much more difficult to predict, identify, and correct the cause of large-scale smart-device failures. De-bugging and re-programming a faulty intelligent device is even more complicated than creating a patch to fight against a malevolent cyberattack because it can be unclear what rules the machines are following.

As a result, no company will be able to recover on its own. To rebound from the potential impact of a cascading set of global AI-related shocks, managers will have to consider the vulnerabilities that exist everywhere from their suppliers to their customers. Addressing those vulnerabilities will require coordination across a large number of technology service providers and other companies that could catch or spread an AI infection to others, regardless of who is at fault.

AI insurance products and services

Insurers should quantify their exposure to a global intelligent device meltdown, offer new products, and advise companies and governments. Even with about $700 billion in capital available in the United States and hundreds of billions of dollars more around the globe, property and casualty insurers' balance sheets are too small to cover all the potential losses from a global intelligent device disaster. But insurers can use data collected on losses across industries to advise companies and governments on how best to quantify their potential exposure to a worst-case scenario.

As they have for natural catastrophes, insurers can also encourage public sector safeguards.

Since insurers cannot completely mitigate the outsized risks posed by extreme weather events, governments of many developed countries and international organizations provide natural catastrophe relief through government agencies like the Federal Emergency Management Agency and public flood insurance programs. Insurers need to help mobilize similar public-sector resources to help the potential victims of an AI-enabled smart device disaster.

In addition, they can start to advise clients on how they can enhance their safety and security protocols to head off the dangerous repercussions of an intelligent device meltdown. Today, some leading insurers are suggesting security procedures that companies could follow to attend to information breaches and interruptions in the event of a global failure of interconnected systems. But they should also begin to explore steps to deal with when smart devices become even more sophisticated and potentially set and follow their own objectives.

AI international protocols

Finally, policymakers should establish international trust and ethics guidelines to govern the development and implementation of ever more advanced AI products and systems. To reduce the future impact from natural disasters, governments and international organizations like the Red Cross and the World Bank collect and share data concerning the destructive ramifications and the support required to help victims. Similar intelligence will be critical to curb the impact of potential smart device shocks as artificial intelligence evolves and the number of connected IoT devices, sensors and actuators reaches over 46 billion in 2021.

About a dozen governments, technology companies and international organizations such as the Institute for Electrical and Electronics Engineers and the World Economic Forum are starting to explore global AI trust and ethics protocols for retaining control of interconnected AI-driven systems and products. These forums are beginning to deepen understanding of the potential harm that intelligent devices could cause and the need for best practices. But much more has to be done.

Establishing the resources required to reduce the risks that will come with the world's transition to more intelligent and interconnected networks will be difficult and costly. But we can't afford not to do it and our experience responding to some of the world's worst "100-year storms" offer a valuable starting point for figuring out how to get ahead of potentially even more severe disasters. We just need companies, insurers, and policymakers to recognize that such efforts are an essential investment in our future. ●

#InfluencerChronicle #AI #MachineLearning #SecurityProtocol

Harvard business review

Can we keep our biases from creeping into AI?

There are two tangible risks in bias when it comes to AI software: AI created with harmful biases built into its core, and AI that does not reflect the diversity of the users it serves.

Not addressing the issues of bias and diversity in AI could lead to a different kind of weaponized AI.

The good news is that AI is an opportunity to build technology with less human bias and built-in inequality than has been the case in previous innovations. But that will only happen if we expand AI talent pools and explicitly test AI-driven technologies for bias.

Eliminating biases in AI: The people

Technology inevitably reflects its creators in a myriad of ways, conscious and unconscious. The tech industry remains very male and fairly culturally homogeneous. This lack of diversity is reflected in the products it produces. For instance, AI assistants like Apple's Siri or Amazon's Alexa, which have default female names, voices, and personas, are largely seen as helpful or passive supporters of a user's lifestyle. Meanwhile, their male-branded counterparts like IBM's Watson or Salesforce's Einstein are perceived as complex problem-solvers tackling global issues. The quickest way to flip this public perception on its head is to render AI genderless, something that could advocate for tirelessly and practice with Sage's personal finance assistant, Pegg.

The more long-term approach requires expanding the talent pool of people working on the next generation of AI technologies.

Diversifying the AI talent pool isn't just about gender. Currently, AI development is a PhD's game. The community of credentialed people creating scalable AI for businesses is relatively small. While the focus on quality and utility needs to remain intact, expanding the diversity of people working on AI to include people with nontechnical professional backgrounds and less advanced degrees is vital to AI's sustainability. As a start, companies developing AI should consider hiring creatives, writers, linguists, sociologists, and passionate people from nontraditional professions. Over time, they should commit to supporting training programs that can broaden the talent pool beyond those who've graduated from elite universities. Recruiting diverse sets of people will also help to improve and reinvent AI user experiences.

Eliminating biases in AI: The technology

Software and hardware engineers regularly test new technology products to ensure they are not harmful to people or businesses that will use them in the real world. Engineers conduct testing in labs and research facilities before a product launches. Ideally, any harmful attributes of the product are uncovered and removed during the testing phase. While that is not always the case, a fundamental and virtually universal commitment to testing does significantly decrease potential risks for everyone producing the products.

The same testing approach is used in the development of new AI technologies. People building AI test their systems for utility, safety, and scalability, with a focus on eliminating product flaws and security vulnerabilities. However, AI is unique in that it typically keeps learning and therefore changing after it leaves the lab.

Currently, though, there is a lack of testing AI products throughout their development cycle to detect potential harms they may do to humans socially, ethically, or emotionally once they hit the market. One way to remedy this is by adding bias testing to a new product's development cycle. Adding such a test in the R&D phase would help companies remove harmful biases from algorithms that run their AI applications and datasets that they pull from to interact with people. → 15

Forrester

Personalized service vs. privacy: when customers want both

Your customers are walking, talking contradictions. Data shows that more than half of them want you to value their time, follow them across channels, and answer their questions quickly and easily.

At the same time, these customers are overwhelmingly worried about how they share personal data – 60% of online North American adults believe or worry that their online behavior is being tracked. Your customers want it all and they want it now, regardless of whether or not it makes sense.

So, given the contradictory and confusing behavior of your customers, how do you walk the line between personalized service and privacy?

In the age of the customer, default to privacy. Offer your customers the option to see exactly what they're sharing with you, and show them how sharing their data will directly benefit them. In 2015, music streaming service Spotify caused a minor uproar by convoluting its privacy policy beyond comprehension. Following the outrage, Spotify released an update to the policy, but the update didn't contain any new information – it clarified what should've already been clear to the average consumer. Use Spotify's example as a cautionary tale; don't wait to be called out on vague and misleading language.

Instead, proactively break down your policies so users can understand what they gain from this exchange: share with us, and you'll get a more streamlined, personalized customer service. Give a little, get a little.

The idea of opening up data policies is not revolutionary. In the early 2000s, Harvard fellow, blogger and journalist Doc Searls began working on a CRM companion known as VRM, or Vendor Relationship Management. He developed this as a model for consumers to manage their end of all interactions with companies. As customers are becoming increasingly aware of how much personal data companies mine from them, a VRM model for service would be a much-needed platform for customers to control access to their data.

Today, if there was a bigger push (and more funding) from enterprises to empower customers with their own data, a VRM model for service would most likely function best as an app similar to your iPhone settings app, or perhaps a browser plugin. Consumers would be able to turn on/off access for every site or company that uses their location services (on mobile or desktop), personal information like addresses, credit card info and phone numbers, and usage of search history for ad targeting.

While customers are existentially worried about their data, they still click through user agreements and may not take action because they feel the problem is too large for an individual to solve. Often, companies take this as a sign that their customers don't care and abuse the data customers reluctantly share. But in the age of the customer, backlash can be swift and devastating. Instead of fighting the tide of customer empowerment, embrace it and be proactive. Transparency and simplicity will go a long way towards establishing trust with your customers. ●

#GDPR #CMO #CIO

CSO:

11 tips for prioritizing security spending

You know all the security advice. You need to have a solid firewall. But it's not enough to defend the perimeter anymore, so you need total visibility into your internal network as well. And don't forget about antivirus. Better make sure it's all in working order by frequent pen testing too! The problem, of course, is that all that costs money.

Figure out what data needs real protection

Not everything on your servers is gold, and not everything requires the same level of defense. Some of your data isn't important, things like user order numbers and other info relevant to internal processing are non-important. Payment information, contact information and any customer personal information should be treated as important. The important data should be kept on a different data store and that should be treated as your sysadmin's personal pet. The non-important data is the cattle.

Start with your company's business goals in mind. Then figure what the most important assets are that support those goals. For example, if you're a retailer, it's imperative to protect customers' payment data and other personally identifiable information. It's equally important that customers can securely transact business on your website at all times to drive revenue.

Take baby steps

It's easy to get overwhelmed by everything you might have to do to get your network up to date. One of the most important things that works well is to break the overall problem down into small, manageable chunks. Focus on small, iterative and testable improvements that over time will add up to a much stronger security posture. You should do your best to focus on one or two things at a time, max. If you're juggling ten different initiatives, then you are spending way too much time context switching and your progress will be minimal.

Embrace autopilot

Anyone who's worked in the IT trenches knows that repetitive grunt work can eat up staff hours. Security shops today are getting killed by the extraordinary amount of tickets and alerts they process to minimize risks. A lot of it is just repetitive questions: how do you do encryption? logging? single sign-on? multi-factor authentication? It takes up a lot of time, so we are moving to an outbound NDA-wrapped self-service portal. Companies no longer have to send someone out to the site, or install anything on the PC. They can avoid spending precious resources for a highly experienced analyst to do the forensic work. Instead, digital tools provide a fast and less costly cyber-response.

Centralize and standardize

Complexity is the enemy of security, to cut down on effort, use a standardized set of security resources, processes, and tools across your organization. To the maximum extent possible, centralize your security defenses with simple, proven, effective controls. When every project uses a different approach, it's impossible to scale assessment and protection.

Gamify pen testing

Just because you can't afford a full-scale simulated hacking from an outside team doesn't mean you should give up on pen testing.

If you have a small team of people and you don't have the resources for penetration testing, a fun team-building exercise is to have a 'hack night,' where you try and compromise each other's code and systems without using your regular admin access.

Pay as you go

Even if you're paying more than $100 a month, an outsourcing deal can substitute a regular recurring fee for large, unpredictable capital expenses. Look to an operating expenditure (OpEx) model instead of capital expenditure (CapEx). Sometimes it's easier on the budget to fund a product or service as OpEx instead of CapEx. Maybe you're paying for a device on site via OpEx or maybe you're buying something as a service. OpEx models allow you to test the waters without huge capital outlay. It's worth asking your vendor if this is an option.

Hack the org chart

Sometimes, what's necessary is to reorient the thinking of people outside IT, and that can make money magically appear for IT security. You could do a quick social engineering test, and that can demonstrate that it's not just machines — it's people being trained properly. If you have an issue with the people being trained properly, that's a pretty solid argument for this as an HR problem. When you shift the focus onto other departments, it shifts focus to that budget as well. The overall goal is better information security, but you have to demonstrate that this is also in other departments' buckets of responsibility.

Follow the money

In fact, a big key in getting cybersecurity funded is not to necessarily present your problem as a purely IT problem. You ask them, if our CRM is hacked, can we do anything as a company? What's the actual cost of every hour that that's down? Then that starts to quantify it and make it a lot easier for top-level people in the company to make choices. If you sit down a CEO and you talk about various attacks and risks out there, then it's not necessarily going to connect with them. But when you say, 'If these systems go down, it costs $X for this amount of time,' that's a standard business conversation at that point — and one that will lead them to make a fairly quick decision. ●

#Security #OrganizationalStructure #Budget #CEO #CMO #CIO

12→ Bias testing would also help account for the blind spots created by the lack of diversity at present in terms of who builds AI. It could help highlight issues which might not be immediately or traditionally obvious to the engineer and, most importantly, to the end user, like how an automated assistant should respond when harassed. Some degree of testing will need to continue after a product is released, since AI algorithms can evolve as they encounter new data. AI-driven technologies will continue to integrate into the everyday lives of people around the world in meaningful ways. It will become commonplace at the office and at home – and not only in the form of voice assistants like Alexa, Siri or Google Home. AI-driven enterprise technologies will improve commercial productivity, close workforce skill gaps and bolster customer experience across industries. That's why now is the right time to implement methods that eliminate harmful biases and take gender out of the equation, expand the population of people working on technologies, and address trust issues with AI. The technology community must do all of these things to make AI's journey into the mainstream one that improves people's lives rather than tearing them apart. ●

#AI #MachineLearning #EthicalAI

Editors note: You will always benefit from a strict ethical way of conducting your business. Of course, it eliminates possible lawsuits when your robot has failed the not so logical human codes of conduct. Even better, an ethical approach (in everything) gives you and your team a magic well of marketing arguments to put out in the air//Johan Lennström.

Atos

Trailblazers create business value from app transformation

As progressive enterprises undertake digital transformation, their focus shifts from IT infrastructure to applications. This is an essential step toward realizing the goal of quickly delivering robust applications based on flexible infrastructure to staff and customers.

Many organizations are undertaking application transformation with little regard to the IT investments that are needed. The shift requires rethinking the way software is built and deployed, and that demands investment.

One of the myths of cloud computing is that it's cheaper than on-premises computing. While that may be true over the long term, organizations shouldn't move to the cloud in pursuit of lower costs. The transition involves both cost and organizational change. Those that don't make the necessary investments in technology and training will miss out on the business value of application transformation.

Some organizations are already well down this path. They all share several characteristics:

- They tend to opt for flexible and secure hybrid cloud environments to give themselves the greatest range of options at the lowest cost.
- They adopt Information Technology Infrastructure Library (ITIL) best practices for service management to keep the IT organization focused on quality of service while also enabling user self-service provisioning and consumption.
- They make extensive use of orchestration and automation for provisioning applications to the business. By removing human operators from routine tasks to the greatest possible degree, trailblazers enable self-service provisioning, reduce wait times, empower business users, and improve business agility.
- They use DevOps agile techniques, which embed development teams into business functions while maintaining close ties with the IT organization. This allows for economies of scale through centralized management, while also enabling greater speed and innovation on the part of developers and their business-side customers.

Having these elements in place enables decentralization of services, improvement of responsiveness, and gain greater visibility and control over their digital investments. The results include more effective asset management, better regulatory compliance, lower cost, and more responsive delivery of IT services directly to the business –critical building blocks of digital transformation.

IDG Research surveyed IT and business decision-makers to better understand the current state of application transformation. It examined the characteristics of those organizations that consider themselves to be ahead of the curve in moving applications to the cloud, and compared their profiles to those that are moving at an average or below average pace.

Companies in the trailblazer group are significantly more motivated by agility and speed to market than their peers. They see the IT organization as an enabler of business transformation more than a steward of infrastructure. They tend to seek dramatic leaps forward in functionality through re-platforming or rebuilding existing applications, a strategic focus that contrasts sharply with the organizations that are adopting cloud simply to save on cost.

Trailblazers also rate the value of cloud computing more highly.

This is especially true for the goal of creating a cloud-friendly culture, gaining visibility into business performance, and creating innovative applications.

Companies that are slow to adopt cloud platforms are often held back by a legacy mindset, and have reservations about modifying existing processes and infrastructure. There's also cultural resistance from people whose jobs will be affected. Cloud is a converged platform that requires managers equally skilled across a variety of technology subjects.

Getting to that model is difficult for many companies because their people pride themselves as being the best in a particular vs. broad areas of the IT stack that is required, but getting people to a converged mindset is critical to cloud.

Convergence also sets the stage for IT organizations to shift their thinking to applications rather than infrastructure. It's about developing and deploying applications and infrastructure in a seamless way. It's a business-centric approach.

Cloud adoption trailblazers take a long-term view of cloud adoption. They accept that cloud platforms are relatively immature, but they believe in the value of the first-mover advantage.

As a result, trailblazers are accelerating cloud deployments faster than companies that are further behind the curve. They have moved a larger percentage of their mission-critical and customer-facing applications to the cloud than the other two groups.

Trailblazers have fewer reservations about making cloud investments and are more likely to have aggressive investment plans for the future because they see benefits across the organization. While a majority of respondents in all groups say they have benefited from improved employee experience, scalability, and agility, trailblazers outpace the others by a significant margin in their perceptions that those benefits are "substantial." They are also more inclined to use cloud for customer-facing applications, which indicates a higher confidence level in cloud as a core platform.

While it's not surprising that trailblazers lead all groups in adoption of public, private, and hybrid cloud platforms, the contrast between the three groups is most evident in use of hybrid cloud, where trailblazers lead by as much as a 2-to-1 margin. In contrast, respondents in the "trying to catch up" category are much more likely than all other groups to deploy applications on-premises.

Trailblazers allocate one-third of their IT budget to cloud migration, compared to 23% for mass movers and just 12% for laggards. Trailblazers also invest aggressively in agile development techniques, and self-service through automation. This satisfies a key requirement of application transformation, which is to put more control in the hands of business users.

In short, cloud is the trailblazer's default platform, with on-premises deployment an undesirable fallback. For companies that are struggling to catch up, the priorities are the opposite.

Security and automation

A perception remains that computing in the cloud is less secure than on-premises, and this was evident in the survey results. Across the board, respondents identify data security as their most significant deployment challenge.

In the case of regulated industries, there are standards in place to make people and companies accountable for how they operate, so that needs to be factored into their journey. Image and patch management can be more complex in the cloud.

Perhaps more importantly, security in the cloud is an outside-in proposition, whereas security on-premises is inside-out. Traditional data centers focus on perimeter security, whereas cloud platforms assume there will be outside interaction.

Businesses are evolving to a customer as a service enterprise enabled through rich APIs. As a result, those APIs need to be monitored and it changes the attack vector.

Trailblazers have overcome security reservations to a greater extent than their peers. Only half identify security and privacy concerns as significant, compared to about two-thirds of the lagging adopters.

→ 19

Gartner

Scaling the enterprise architect role

Gartner's predictions indicate that the role of the enterprise architect, EA, and technology innovation leader is scaling in terms of:

- Supporting strategic planning for both the business and IT
- Focusing on digital technologies within the business ecosystem
- Enhancing integrated business and technology skills to deliver the role in the next decade
- Adopting different tools for analyzing the interrelationships and inter-dependencies of changing plans, in-flight projects and the state of existing assets over time.

90% of enterprise architects are involved in technology innovation. Furthermore, 90% of those engaged in technology innovation are focused upon the marriage of new technology to new business models. 63% are engaged in their organization's business strategy planning. For those who have been in EA for a long time, these are heady days for enterprise architects. In our 2017 survey, we found that 68% of heads of EA report directly to a C-level executive, including to the CIO (45.7%), CEO (5.4%), CTO (16%) or CFO (1%). The "seat at the table" many dreamed of a decade ago is there, and filled with savvy and eager to help leaders.

Important recommendations

Amongst the numerous recommendations in the report, for EA in the future, those are imperative:

- Upskill the role to support leadership expectations in the next decade. Become more fluent in business strategy and business model techniques and terms, as well as your own business strategy and model. This may mean investing more in business architecture skills and capabilities, as well as partnering with business strategy leaders in the organization.
- Expand capabilities with millennial enterprise architects, as baby boomers exit the workforce.

Technology still counts in the future, but it counts more when it's directly applied to the delivery of a business outcome. Innovation planning, monitoring in-flight projects, and assessing the fitness of current state assets are not done in a vacuum when done with desired business outcomes set before you.

Expect expansion of skills and capabilities in the role of EA, complemented by transparent governance and supported by the rise of new tools in support of a new digital, business and IT ecosystem. The themes of tools, strategy, skills and digital business continue to shape the role in the coming years.

- 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.

Predictions about EA in 2020-2022

- By 2020, 55% of organizations will have a continuous, and integrated, business and IT strategy planning effort.
- By 2020, 75% of the heads of EA will be a key strategic business and technology advisor for a CxO.
- By 2022, 80% of successful organizations will rely on EA to orchestrate digital business ecosystems and digital platforms.
- By 2020, EA efforts that focus on enabling investment decisions with transparent governance will double their business value.
- Through 2020, 55% of EA teams will focus their business ecosystem, but less than 10% will be able to analyze their ecosystem. ●

#EA #EnterpriseArchitect #InfraStructure #CTO

17→ In fact, many trailblazers report that the enterprise-grade security cloud providers deliver is more of an asset than a risk. This positive attitude enables them to move ahead with cloud deployment more confidently, and with a wider range of applications.

The technology of orchestration and automation is actually the easy part, the bigger challenge is the organizational transformation that companies need to get through to realize a new way of building and deploying applications. Unfortunately, in many lines of businesses, the application developers and infrastructure teams are still separate.

Exposing services through APIs minimizes custom coding, enables reusability, and supports automation. Ideally, there's a master orchestration platform that's aligned with the business process.

In line with that, trailblazers are significantly more likely to adopt ITIL processes than mass movers and those trying to catch up (33% to 23% and 14%, respectively), and more than twice as likely to have adopted those service management standards than laggards.

This means they manage at a higher level, with less concern about the details of infrastructure. Automation frees them to focus on the business. It also enables them to adopt DevOps for cloud-native development by a nearly 3-to-1 margin compared to others.

DevOps intrinsically involves end-user customers more directly in defining outcomes, creating closer alignment between applications and business value.

Although many organizations are first attracted to cloud by the promise of reduced cost, those that have made the transition see the payoff more diffusely. Across the range of respondents, cloud adopters say the greatest benefits they've seen are: creating a cloud-friendly culture that stimulates new roles and skills; improved availability; application innovation; and improved visibility into applications and the development lifecycle. Cost controls came eighth on the list.

Organizations that have amassed considerable experience and made large investments in application transformation are also significantly more optimistic about the potential of the cloud, and are accelerating their transitions accordingly. As they become more reliant on the cloud as a core application platform, they exhibit greater confidence in a "cloud-first" strategy. Trailblazing organizations are more likely than others to adopt associated cloud-native practices such as DevOps and automation. This enables them to realize agility and cost-saving benefits at a more rapid pace than their peers.

Trailblazers show a greater willingness to take on the investments and organizational change needed to deploy flexible architecture. They see the benefits as going far beyond cost savings to include business agility, speed to market, efficiency, and employee engagement. They understand that migrating to the cloud is as much an organizational and cultural shift as a technical one. But they also see the ancillary benefits of embracing other technical disciplines that cloud migration enables, such as ITIL and DevOps.

As a result, trailblazers are more tightly bound to business goals and culturally committed to business outcomes. They're probably also likely to have more motivated employees.

As a result of all of these factors, trailblazers are more likely than late adopters to facilitate successful application transformation. As they accelerate their transition to cloud platforms, their lead over others on the continuum will continue to grow. Followers can close the gap by moving quickly to make the necessary financial and cultural commitments. ●

#Cloud #Digitalization #Management #Devops #Infrastructure

CIO

Hybrid IT security

Cybersecurity is no longer a layer that's added at the end of a project. An increasingly sophisticated threat landscape and more distributed IT environments are forcing organizations to ensure that security is baked into all aspects of their Hybrid IT models, from on-premise systems to cloud applications.

A secure, resilient infrastructure is vital to reduce risk and increase the reliability of mission-critical systems and applications.

Security has become the top priority for IT projects. In the next 12 months, 60% of enterprises plan to increase spending on security technologies as they try to reduce the risk of an attack that could disrupt operations and lead to significant financial loss or brand damage.

Rising threats have led many organizations to integrate security tightly into their overall IT strategies across all platforms and systems, and down into functions such as software development. More than half (51%) of CIOs in the 2017 State of the CIO survey said security is now an integral part of IT strategy – up from 37% in 2016. In heavily regulated industries such as healthcare and financial services, those percentages are much higher (68% and 64%, respectively).

Whenever you make your environment more complex, there's the potential for more mistakes. Ultimately that is the driving force behind dev-ops/no-ops in this whole space. As your environment gets more complex, the old ways just don't scale.

A comprehensive security and governance audit is a critical first step in shoring up Hybrid IT security practices. The audit should include an evaluation of all policies and user privileges, as well as of where and how data is stored throughout the organization.

End-to-end visibility will allow security teams to introduce the right mix of security layers and controls to ensure redundancies and create protections across the entire infrastructure.

Data-centric security techniques, combined with identity-based controls, are gaining traction as better ways to defend against unauthorized access to information and systems across environments. Companies are deploying advanced encryption techniques to protect data at rest, in motion, and in use across public and private clouds and enterprise systems. Identity management adds an additional layer of role-based access rights across service catalogs and enterprise directories. ●

#Cloud #Hybrid #Security

Executive Report

P.t. Editor-in-chief: Johan Lennström, johan.lennstrom@executivereport.se

Publisher: Emilia Romboni, emilia.romboni@executivereport.se +46 (0) 73-615 10 20

Business manager: Andreas Romboni, andreas.romboni@executivereport.se

Subscriptions: pren@executivereport.se

Head of operations: Emilia Romboni, emilia.romboni@executivereport.se

Mailing address: Executive Report, Hökartorget 5, 776 30 Hedemora, Sweden

Produced by: Formspråk Dalarna / Brandfactory