Master Your Environment: 6 Key Changes in IT and How to Use Them to Your Advantage

Change is widespread

New technologies and applications are generating marked pressures to modernize and transform IT. Business and IT leaders undoubtedly sense this, but even industry outsiders are feeling ripple effects. Cyberattacks have impacted the large majority of consumers, compromising the privacy of their data and personal information. Automation is being portrayed by media outlets as a top threat to jobs and job security. Cloud providers are dominating global financial markets.

Although the changes are indeed widespread, it's important to distill the activity into digestible bits. What patterns are occurring? What impacts do they have? How does each area of change relate to others? Answers should inform IT leaders — Cloud + Data Center Transformation (CDCT) helps clients take action on these answers through our IT transformation services.

Six IT changes you need to know about

CDCT Chief Architect Juan Orlandini clarified six major shifts, or "buckets of massive change," in a recent video. This list effectively helps us contextualize and organize the movements within IT today. In this whitepaper, we will elaborate on key changes and how each is compelling leaders to drive comprehensive IT transformation to stay relevant in this new age.

The changes are:

1. Cloud is proving to be more complex than expected — and, more hybrid.

2. Containerization has become a critical tool for productivity and innovation.

3. Security is no beginner's game, requiring advanced strategies that can prevail in an age of ultra-interconnectedness.

4. Automation is enabling unprecedented efficiencies and opening up new competitive chasms between laggards and leaders.

5. Artificial intelligence (AI) and deep learning mechanisms are perhaps the best tools available for extracting value out of our data.

6. Network transformation is a necessary consequence of responding appropriately to the five other changes.

Change 1. Cloud

It's true that "you don't know what you don't know." When cloud became commoditized, options followed — Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Cloud could purportedly handle the entire IT stack better and cheaper. Entire IT operating models were spun on their heads. A revolution had begun.

Today is a different story. IT organizations have been to cloud and back, and everywhere in between. The notion of "lift and shift" is evidently fallacious. Data strategies that accommodate both the technical and financial requirements of an organization are difficult to devise. On-premises infrastructure is still necessary and/or desirable for many, if not most, businesses for its ability to better handle compliance requirements, data volume and storage, specific security needs, and so forth.

In order to maximize specific benefits of each platform — cost, efficiency, security, etc. — hybrid cloud is an obvious and pragmatic option. It can also be a key to competitive advantage. According to the Insight-commissioned IDG Survey, "The Challenge of Change: IT in Transition," organizations who have made the most systemic progress in terms of IT transformation are using a hybrid cloud approach.

However, knowing a hybrid cloud model may be optimal still leaves a large gap between strategy and execution. Business and IT leaders need to navigate the many challenges: assembling accurate technical requirements, selecting a cloud provider, developing effective governance and processes, and so on. It is often for reasons like these that businesses look to a firm like CDCT, who can help them clarify, define, and implement an appropriate cloud strategy.

Change 2. Containerization

Virtualization isn't a new concept nor practice. Moving workloads from physical systems and hardware to virtual environments has been popular for decades. But containerization delivers another level of abstraction and, thus, more potential benefits.

Containers are lightweight and developer-friendly, made for packaging and deploying modern applications. They can run almost anywhere — Linux®, Windows®, macOS®, virtual machines (VMs), and/or bare metal. Think of containers as pre-bundled runtime environments, fully inclusive of an application and its dependencies. They're equally suited for on-premises and cloud platforms, which is great news for organizations implementing a hybrid cloud strategy.

There are always tradeoffs, though. The container ecosystem cannot exist without making substantial adjustments in terms of software development and delivery. IT organizations have to retool, retrain, and refactor to evolve from a traditional to a container-compatible, DevOps approach. At the same time, core concerns do not vanish. Applications still need to be scalable, run on up-to-date software, managed with effective governance and controls, and able to provide visibility.

Change 3. Security

There isn't an IT professional out there who isn't nostalgic for the days where a good firewall was sufficient protection. If only that were still the case today.

Why isn't it? There are obvious and non-obvious reasons.

There are more inroads and backdoors.

- Everything has become digitized. Compute is everywhere, from the factory floor to the customer experience, from expanding IT organizations to IoT devices. Data is ubiquitous and extremely valuable. And, we're more interconnected than ever before. Events like WannaCry and NotPetya are unfortunate demonstrations of our extensive linkages (and vulnerabilities). Organizations like Equifax know all too well the costs and aftermath of attacks.

We use more technologies — and have more silos.

- In sharp contrast to our interconnectedness as a whole, are the organizational silos that have arisen out of piecemeal IT improvements or updates, or just plain shadow IT. One example: an IT organization is cloud-resistant, but the customer-facing divisions opt to use unsanctioned cloud applications anyway. Who manages these new cloud-based tools if IT isn't even made aware of their use? Who's responsible for securing the environment? Comprehensive and well-integrated security strategies have never been more in-demand.

Threats have metastasized accordingly.

- Cybercriminal tactics like malware and phishing have been in practice for some time, but we can now add to the list demons like distributed denial of service (DDoS) attacks, "man in the middle" attacks, cryptojacking (cryptocurrency generation using hacked computing resources), etc.

Working with a team like CDCT can be beneficial because we provide not only technical expertise of advanced security tool sets, but also business and change management acumen. This enables us to recommend systematic improvements to the entire security ecosystem that are tailored for unique industry or company dynamics.

Change 4. Automation

If complexity is a modern problem, automation is its antidote. Automation can mean robotics, analytics, "smart" products, software, supply chain improvements, or anywhere that efficiencies can be found. In the case of our work at CDCT, it can also mean automating infrastructure and eliminating manual steps to make sure that systems are easier to deploy, maintain, and troubleshoot. Automation is being hailed as a key tool, in addition to human-based efforts, to strengthening security. Automated patching of hardware, software, and databases is now being used by a growing number of companies.

But when we talk about automation, it's become critical to view it within the same framework as IT transformation — relating to people, processes, and technology. Take legacy infrastructure management, for instance, in which tasks are manually performed and silos abound. It makes no logical sense to even imagine a technology that would singlehandedly modernize this scenario. Automation offers ways to assemble infrastructure on-demand out of disaggregated components. But that's only part of the solution.

What skills are needed to make a change? Do those roles exist currently? If not, do you train up or hire? How do you confidently unite the objectives and initiatives of multiple business units into a singular vision? The point is that automation drives corollary change in people and processes, as well. Groups like CDCT can play a crucial role as a strategic partner to help firms leverage automation in ways that are optimized for specific business needs and characteristics.

Change 5. AI

For some, the advent of artificial intelligence (AI) is a massive change in itself. Indeed, deep learning and AI are creating tidal waves of disruption that are surpassing our collective imagination. The key driver? Our vast supply of data. Extracting value out of data is easy when it fits within a single spreadsheet; when data spirals out to data-lake size, primitive analytic tools begin to look better suited for a caveman.

The use of AI is growing at exponential rates, impacting nearly all IT organizations and business functions. To illustrate our point, here are three strategic planning assumptions published in Gartner's "Predicts 2019: Artificial Intelligence Core Technologies. [1]"

"**Through 2023**, computational resources used in AI will increase **5x** from 2018, making AI the top category of workloads driving infrastructure decisions."

"By 2023, **70%** **of AI workloads** will use application containers or be built using a serverless programming model necessitating a DevOps culture."

"By 2023, **40%** of I&O teams will use AI-augmented automation in large enterprises, resulting in higher IT productivity with **greater agility and scalability.**"

Nearly every massive change discussed in this whitepaper gets a mention within the conversation of AI. Of course, this goes back to data. We've entered an era where our data decisions — how we store, manage, protect, analyze, and exploit data — are really strategic business decisions. An experienced partner like CDCT can play a pivotal role.

Change 6. Networking

Innovations in networking technology have reinvigorated this IT domain, providing novel solutions to long-standing problems related to cost, complexity, scalability, and security. As always, networks facilitate intercommunication between enterprise components, corporate users, and customers, however the explosion of complexity and data volume has challenged legacy models of networking and forced manufacturers and end users alike to adapt. Your AI engine has to connect to your all-flash storage arrays. Your container engine and compute infrastructure need to be able to move workloads from one site to another. Your users need optimal traffic path to their local Azure® or AWS® point of presence for some traffic, but otherwise need to be directed through corporate hub sites for security policy enforcement. Campus networks need ways to dynamically identify and segment connected hosts by policy, without human intervention.

Organizations need to prepare their networks for secure, compliant cloud connectivity. Network and security administrators need to know who and what is on their network at any given time, no matter the platform, endpoint, or application. But achieving these goals sometimes seems like a pipe dream in modern enterprise environments. Typical large enterprises have millions of endpoints, and billions of network security events every month. Annual global cloud IP traffic is skyrocketing to the tens of zettabytes within the next couple of years. Attaining or maintaining compliance with statutes like HIPAA, PCI, GDPR, and NIST introduces another layer of demand and complexity. Throughout all of this, the network remains a fundamental component underlaying all of the organization's infrastructure. These new technologies, demands, and business processes are forcing organizations to rethink their approach to networking and security — and what problems networking technology can solve.

When the going gets tough

The changes we've discussed are creating exciting opportunities for businesses to transform to meet modern demands. IT pressures are now three-pronged — internal (keeping the lights on); external (needing to innovate, differentiate, and compete); environmental (taking action in response to the six massive changes).

Cloud + Data Center Transformation is here to help. From targeted assessments to consulting engagements, technology selection to infrastructure optimization, cloud strategy to transformation, we help bring your unique environment into the modern era.

Watch the video with CDCT Chief Architect Juan Orlandini reviewing the six major changes shared in this whitepaper.

Learn more with these resources:

- Comprehensive Cloud Strategies and Solutions
- Infrastructure Strategy Workshop
- Transforming Network Security: How to Win Against Cyberthreats
- Software-Defined — 4 videos

Meaningful solutions driving business outcomes

We help our clients modernize and secure critical platforms to transform IT. We believe data is a key driver, hybrid models are accelerators, and secure networks are well integrated. Our end-to-end services empower companies to effectively leverage technology solutions to overcome challenges, support growth and innovation, reduce risk, and transform the business.

Learn more at:
insightCDCT.com | insight.com

1. Gartner Predicts 2019: Artificial Intelligence Core Technologies, Chirag Dekate, Erick Brethenoux, Jim Hare, Arun Chandrasekaran, Milind Govekar, and Charley Rich, November 29, 2018.