Agents of Change: CIO Priorities for 2016

Practical Perspectives and Advice on Today’s Most Impactful Trends from VMware Transformation Experts
Introduction

Today’s most successful enterprises are transforming themselves, upending business models, disrupting markets. What’s more, they’re turning on a dime—and the pace at which they’re doing so is only increasing. For these winners, that agility translates into increased customer satisfaction, better margins, and higher sales. For their IT functions—responsible for so much of this new flexibility and speed—transformation drives a new relationship with the business. IT is now a fundamental and ongoing contributor to accelerating business value.

As CIOs look to transform their own IT organizations in year ahead, their greatest challenge lies in delivering that change in an environment that is itself fast moving.
In 2016, IT can only expect increased pressure to deploy continuous innovation to capture both business value and further efficiencies.

Our experts see this daily as they work with customers around the world, gaining insight into the challenges that companies face and the strategies that are working on the transformation frontlines.

In 2016 we expect several specific phenomena to shape the development of IT organizations this dynamic environment. The following chapters explore three main trends that we believe CIOs need to be aware of as they consider embarking upon, or continuing, transformations of their own:

- Companies are looking to scale DevOps beyond individual application pipelines and pilots.
- IT needs to be able to work at multiple speeds. It’s all about being multi-modal.
- Security offers a challenge, but a major opportunity, too
Putting DevOps into Practice

In 2016, as companies push further into their IT transformations, many will be looking to scale up “DevOps” approaches that they have already adopted on a limited basis across their entire IT organization.

The argument for DevOps is well established: **DevOps dramatically increases the speed at which IT delivers applications to the business.**

What exactly is DevOps, though? In our work with stakeholders across the IT spectrum—in applications, infrastructure, service, and program management—we’ve found it means something different to each group.
But where they’ll agree is that DevOps is primarily a culture—one that emphasizes collaboration and communication in software development and that aims, as much as possible, to automate the process of software delivery.

Beyond speed, DevOps has other benefits. Greater automation and faster feedback also improve quality, because defects are spotted and fixed faster. DevOps results in a product more likely to meet actual customer needs. It signals that you “get it,” heightening your appeal to talented and ambitious potential hires. And in the longer term, investment in automation results in serious cost-savings.

But the overwhelming appeal behind DevOps is in meeting customer needs more quickly, and thereby directly impacting business value. Using a traditional approach, one VMware customer was taking up to nine weeks to deploy changes to a customer-facing application with millions of users.

After adopting a DevOps approach, the IT organization was deploying those changes within ninety minutes.

More and more businesses are taking note, often after seeing DevOps cultures thriving in smaller and newer competitors.
Until 2015, though, there was still a sense that DevOps remained a play for the scrappy little guys and for just a part of the IT function: the software application team. But over the last year, larger companies (like Comcast) and companies in more traditional sectors (like Capital One), have adopted DevOps practices more broadly and gone public with their results, spurring more companies to push a DevOps approach across their IT organization.

**DevOps in 2016—making the move across IT**

In 2016, we expect this trend to continue—businesses will increase pressure on their IT functions to provide the delivery times they are seeing in their nimbler competitors, driving a DevOps approach beyond application development (AppDev) into the rest of the IT function, especially teams responsible for infrastructure and operations (Infra/Ops).
It will be increasingly important, therefore, for the AppDev and Infra/Ops teams to work more closely together, with pressure for cooperation coming mostly from the application development side, to ensure that investments made in infrastructure and platforms get fully used.

**Application development organizations** are the most likely to be onboard with the DevOps model already. Custom application teams are commonly adopting some kind of agile delivery model, establishing new development frameworks and infrastructure platforms that allow for even faster and easier development.

They are also reassessing their organizational structures to ensure that they have the right people and skills to support the creation and ongoing support of “cloud native” applications in a continuous delivery operating model.

Many packaged application teams, meanwhile, are exploring the use of DevOps practices to continuously release new application modules, customizations, and integrations.

**Infrastructure teams**, in many ways, face a bigger challenge. Both business units and application teams are pushing them to deliver at a faster pace while also being more flexible and secure in how they operate and manage the platforms they engineer. That’s driving infrastructure leaders to look seriously at adopting DevOps best practices from the software development community, including strong versioning and testing practices. Ultimately,
they will need to establish DevOps for their infrastructure and platform services, but in a way that accommodates legitimate concerns about stability and legacy systems (see the following chapter for more on this).

In the face of these pressures, it’s essential that CIOs encourage the entire IT team to embrace the need for change.

That extends to the structuring of employee teams. We have seen some customers establish a separate DevOps team between development and operations, which simply creates a new hand-off function and silo.

More successful organizations instead focus on developing a streamlined flow across teams that lets them build applications quickly and run them easily on their cloud.

DevOps is changing the way infrastructure is being consumed.

The pressure on application teams to speed delivery is driving them to access infrastructure and platform services in ways that can be more tightly integrated into a fully-automated delivery pipeline. That can happen in a number of ways:

- infrastructure-as-a-service
- platform-on-demand (i.e. using a SQL or WebLogic server)
- a full-blown platform-as-a-service (i.e. Cloud Foundry)
- a service for executing containers
Choosing and providing the right option will be a major preoccupation for many CIOs in the year ahead (see the following chapter for the multi-modal aspect of this trend).

But the reality is that any one path is unlikely to provide everything an organization needs, thanks to variations across application types and teams.

Flexibility therefore remains key. In old-style Infra/Ops you typically made a plan, executed on it, and were done. But a significant part of applying DevOps thinking across the IT organization in 2016 will be to encourage an overall mindset of continuous delivery and improvement. CIOs need to expect to keep innovating at the speed of business, and therefore to revisit the decisions they make in optimizing today’s pipeline as customer needs change.
Multi-Modal Along the Path to Bimodal

When it comes to the specific challenge of transforming IT Infrastructure & Operations (Infra/Ops), a major 2016 trend will see businesses moving faster towards Gartner’s model of Bimodal IT, initially doing so by implementing a multi-modal approach where IT runs in both modes, traditional and agile, at one time.

Generally, this will be accomplished through a “greenfield” implementation of an Infra/Ops organization and operating model, enabled by a software-defined data center-based infrastructure.

That’s a shift from how changes in Infra/Ops organizational and operating models have typically been undertaken. But companies have found it much harder than expected to achieve the IT operational agility they need.
In response, they’ve taken advantage of new, software-defined data center-based cloud infrastructures to implement a new Infra/Ops organization and operating model focused only on their new cloud infrastructure. This model is designed to begin small but then be expanded and enhanced as the scale, number of new services, and business criticality of their clouds increase.

Their intention is to then migrate the traditional Infra/Ops organization to the new operating model approach over time, having refined and validated the new model in support of their cloud services first. We expect this approach to become increasingly accepted and adopted in 2016.

This new Infra/Ops organization and associated operating model is a hybrid of Gartner’s Bimodal IT. It embraces Gartner’s Mode 2, which emphasizes agility and speed, but still provides the key benefits of Mode 1, which prioritizes production reliability and predictable performance, while also meeting (and influencing) security and compliance requirements.
Multi-modal IT in practice—new roles and team practices

At its core, the new, multi-modal Infra/Ops organization is both service- and business-centric and features some very specific new roles. It includes, for example, a business relationship manager role within IT, responsible for working closely with, and intimately understanding, IT customers' business requirements and their predicted demand for new and existing services consumed from the cloud that IT provides.

Each service, meanwhile, has a service owner responsible for the lifecycle of, and satisfaction with, that service. That person is responsible for taking an outside-in, customer-centric approach, actively involving all stakeholders in service definition and managing a tight feedback loop as service capabilities are delivered and refined. Service investment decisions will be made via a more business inclusive portfolio management process.

The Infra/Ops teams in the new Infra/Ops organization will exhibit new structural, technical, and cultural characteristics that reflect their new approach to operations.
Structurally, the Infra/Ops teams will be:

- Increasingly virtual, collaborative and fluid while being aligned to services – whether the service is providing (and running) underlying infrastructure services to other service teams or for consumption by end customers directly.

- Moving away from the traditional plan-build-run paradigm as an organizational construct into teams responsible for all three throughout the lifecycle of the service(s) for which they are responsible, and delivering those services using an agile model with continuous delivery of service capabilities.

- Directly involved with the business and other IT stakeholders in the definition of the service for which they are responsible.

- Fluid but with some permanent core roles. Subject matter experts will float in and out as needed during service capability delivery sprints. Permanent core roles will collaboratively address day 2 operations while innovating and continuously delivering new operational capabilities.
Beyond displaying increased shared technical competencies pertinent to their roles, all organization members will need to show they:

- Are entrepreneurial self-starters able to balance the need for innovation with operational reliability.
- Have a systems-thinking mindset.
- Understand the need for continuously learning and expanding their skills.
- Possess the software development skills to take an “automation-first” approach when appropriate.

From a cultural perspective, all team members need to be focused on team results that provide value to the business rather than solely within IT. They:

- Take “controlled risks” while achieving results.
- Have a “change is the norm” mindset, embracing the chance to enable and accelerate the pace at which the business can change.
- Are equally comfortable working with internal and external cloud service providers.
- Promote collaborative global standardization with regional execution to achieve global efficiencies and consistency in service delivery.
A model that works

Companies are adopting this approach to multi-modal IT because it delivers both the agility and measurable, added value that businesses are looking for without sacrificing the stability that they require.

We expect its popularity to increase through 2016 and spur a further acceleration in successful and sustainable IT transformation initiatives.
A New Hope for Security

For all the agility they bring, cloud technologies add a new dimension to IT security risk.

After all, business users can now provision their own cloud infrastructures without paying attention to internal corporate security guidelines. Fast cloud provisioning also often leads to a proliferation of “temporary” workloads—many of which are not rigorously controlled.

And cloud data can be stored anywhere, including in nations with very different regulatory expectations, making global protection a challenge.
Yet until recently, security has been an afterthought for many IT teams, even as they have adopted cloud-based solutions. When they do think about security, many CIOs are concerned at the prospect of placing security barriers in applications or processes that slow them down at a time when speed is more important than ever. The result: frequent, avoidable security breaches that result in financial and reputational damage.

For 2016, then, a top CIO priority will be to make security a core competency—both by taking steps to integrate best security practices into their transformation plans, and by taking advantage of new technologies like software-defined security and micro-segmentation that can increase both security and speed at the same time—placing the organization, for once, ahead of the bad guys.

Here are four ways in which CIOs can reset the security conversation and expectations across IT:

1. Build a broad awareness and knowledge base.

All IT team members should understand the basics of security. That includes both the enterprise's own security policy and a broad awareness of relevant laws (e.g. data protection) and compliance requirements (e.g. PCI, Sarbanes Oxley). It also helps to build awareness of security breaches that are common in the market sector being addressed.
2. Break down technical silos

Technical silos occur naturally as employees organize around common skills, but they can lead to serious gaps in security coverage. Hackers are experts at finding those gaps, through which they can then launch intrusions. To avoid this, IT needs to consider security end-to-end and assume that breaches can occur in any layer of the infrastructure. Just as modern IT services are designed end-to-end across silos, IT teams need to work collaboratively across functions to manage security risks.

3. Involve business stakeholders

Transformational IT builds a strong working relationship with business stakeholders, and that can have a direct, positive impact on security. With a Multi-modal and DevOps approach, IT roles will already be more closely tied to the business (e.g. Service Owner, Customer Relationship Manager etc.). Security should a key part of this cooperation, helping to:

- Establish clear responsibilities (Who patches the workloads? Who checks compliance?).
- Assign a security champion whenever undertaking a virtualization project.
- Document responsibilities and expectations (e.g. within the service level agreements).
- Ensure regular communications about security between business users and IT (Are there security-critical applications? Confidential data? What level of confidentiality?).
4. Automate day-to-day security & compliance checks.

Increased automation, and the benefits derived from it, are an essential part of the transformation story. IT should use automation and operations management tools to configure and leverage its security and compliance procedures, too. It builds security into applications from day one, avoiding issues that otherwise consume effort and attention, and addresses the fear that security measures slow speeds—instead, security policy automation increases efficiency and frees up employee time to focus on the bigger security picture.

To that end, IT should:

- Ensure that provisioning blueprints match the latest security policies.
- Configure management dashboards to display an aggregate view of compliance risk across your virtual infrastructure.
- Automate and report on compliance checks.
- Leverage automated integration with the support desk so that risk issues are acted upon.

IT can do more, though. By leveraging new technical models and adopting a new security mindset, it can significantly improve the defensibility of its data networks.
Shifting the paradigm on network security with micro-segmentation

The traditional approach to securing cloud-based networks is to setup strong security firewalls at the perimeter. This is the fortress model of security – highly protected boundaries and a gate to control traffic at the entrance.

But even the best-constructed firewall should be assumed to be breachable, which means that intrusions need to be anticipated and planned for. Here the fortress model falters.

Once a network's perimeter is breached and a first workload compromised, intruders can compromise other workloads with little challenge and then locate potentially sensitive data to retrieve. There may be other lines of defense within the fortress, but these tend to be static, and once broken face the same problem of lateral mobility.

The most powerful response to this is micro-segmentation. Micro-segmentation allows fine-grained network security that can prevent not only the initial intrusion, but also attacks at the other stages since it isolates workloads. The would-be intruder is as challenged in moving from one ‘room’ to the other as getting past the entrance in the first place.
Just as importantly, **micro-segmentation** allows security policies to be tailored to individual workloads. Network security rules can be associated with any logical object. When the workload is moved from one network location to another, those security rules are maintained, rather than remaining attached to a workload linked to a fixed network address. (Micro-segmentation also frees up developers to be more aggressive in introducing changes, since individual application failures are far less likely to cascade, so there’s an agility benefit too).

Leveraging this potential, however, requires a new mindset as outlined in the introduction above—shifting from a static security model to dynamic, fine-grained security.

It also requires the cloud team to develop new skills and deemphasize old ones. Routine configuration skills can be replaced with automation, for example, but traditional network skills need to be complemented with added skills in design and programming.
Conclusion—Make a Plan, Make Your Case, Find Help if You Need it

For CIOs who are ready, the key waypoints on the path to transformation are unchanged, although we see one or more steps left out by CIOs surprising often:

- First create a compelling picture of what success will look like—not just for IT, but for the business as a whole. Drawn well, this makes the case for transformation clear, and offers a vision around which to rally employees concerned at the prospect of change.

- Next comes the roadmap. How will the organization get there? It’s wise to take a cue from DevOps practice here: smaller, incremental phases produce value faster and build more momentum than larger but less frequent jumps.
After that, the plan—ambitious, inspiring, and also entirely achievable. It needs to detail the capabilities required in the transformed organization, and how, exactly, they will work to meet your goals.

Helpfully, the business case for transformation is getting ever stronger. Although companies figure ROI differently, many are seeing 20% to 25% cost savings from adopting a software-defined data center approach that maximizes automation and orchestration—making IT transformation self-funding in very little time. Savings come both from reduced operating costs (fewer staff, lower software fees etc.) and reduced/avoided capital outlay (hardware).

But more than ROI is at stake here. The real win from IT transformation is the new business value it creates.

As CIOs plan for the coming year, they should figure the additional revenue that increased velocity and agility will bring their business. That means predicting how much their market share can be expected to grow, and placing a financial value on the benefits of better knowledge management, faster training times, and having more consistent, auditable, and standardized systems in place.
In 2016, CIOs will be under increased pressure to progress along this path both sooner and faster. Understanding the specific trends in DevOps, Multi-modal IT, and security management outlined above will be key to developing plans most likely to result in transformation at the pace that is expected of IT today.

At the same time, most IT organizations will likely be bandwidth-constrained simply from running their everyday operations and won’t have the time or expertise to plan and manage a successful transformation alone.

Throughout this process, then, CIOs should be sure to secure the guidance and help they need. Luckily, the case for securing outside partners in 2016 is simple: a do-it-ourselves approach can extend a transformation timeline by years, in an environment where no business can afford to give IT that time in which to change.
About VMware Professional Services

VMware Professional Services transform IT possibilities into business outcomes. Our comprehensive portfolio of consulting and education services help you uncover and exploit the unique opportunities made possible by VMware technology and solutions.

Drawing on our unparalleled product expertise and customer experience, we collaborate with your team to address the technical, people, process, and financial considerations for your VMware solution to deliver results that are positive, tangible and material to IT and your business.

For more information on VMware Professional Services and how we can help you, contact your local VMware representative or visit www.vmware.com/consulting.

Additional Resources

- CIO Vantage Blog
- Accelerate Advisory Services Blog
- Operations Transformation Services Blog