ESG

Enterprise Strategy Group | Getting to the bigger truth.™

Technology Showcase

The Silent Threat of Configuration Drift

Date: May 2019 **Author:** Scott Sinclair, Senior Analyst

Abstract: In the digital economy, the drive for success amplifies the pressure placed upon IT. As demands scale (often well beyond IT personnel resources), shortcuts and ad hoc enhancements become common. As a result, infrastructure configurations can drift away from best practices, creating gaps which, at best, limit efficiency. At worst, they introduce security gaps, downtime for critical applications, and business risk. Tools that can automatically identify and address the often-hidden threat of configuration drift are vital to IT success in the modern digital age.

Introduction

Data and IT services are the fuel for modern business. Seeking superior returns, companies increase investment to support digital creation and usage. They hire individuals who have greater digital demands. These people now generate more data, store more data, and use more data. Data has become entrenched in every portion of modern business, creating not just opportunity, but also risk.

As data becomes intertwined with essential business operations, assurance of IT services continues to be job number one. For example, 40% of IT decision makers identified improving security/risk management as a top-five justification for IT investment over the next 12 months.[1] While the fundamental need for IT stability is nothing new, data's recent role as a revenue driver has altered the grading scale for modern IT organizations.

One in four (25%) line-of-business executives involved with IT decisions considers their IT organization a business inhibitor. A commonly identified rationale for this negative designation: IT organization's processes to deploy IT services take too long (cited by 32% of respondents).

For a modern business, resiliency cannot be compromised. But speed is of the essence. As demands mount and infrastructure scales, traditional (often manual) tools often can't keep pace. As IT attempts to accelerate traditional processes, teams take shortcuts—and new threats, such as configuration drift, are thus introduced.

Addressing those threats while accelerating IT is essential. And understanding how a new technology can assist in identifying and addressing configuration drift should become part of any infrastructure technology evaluation.

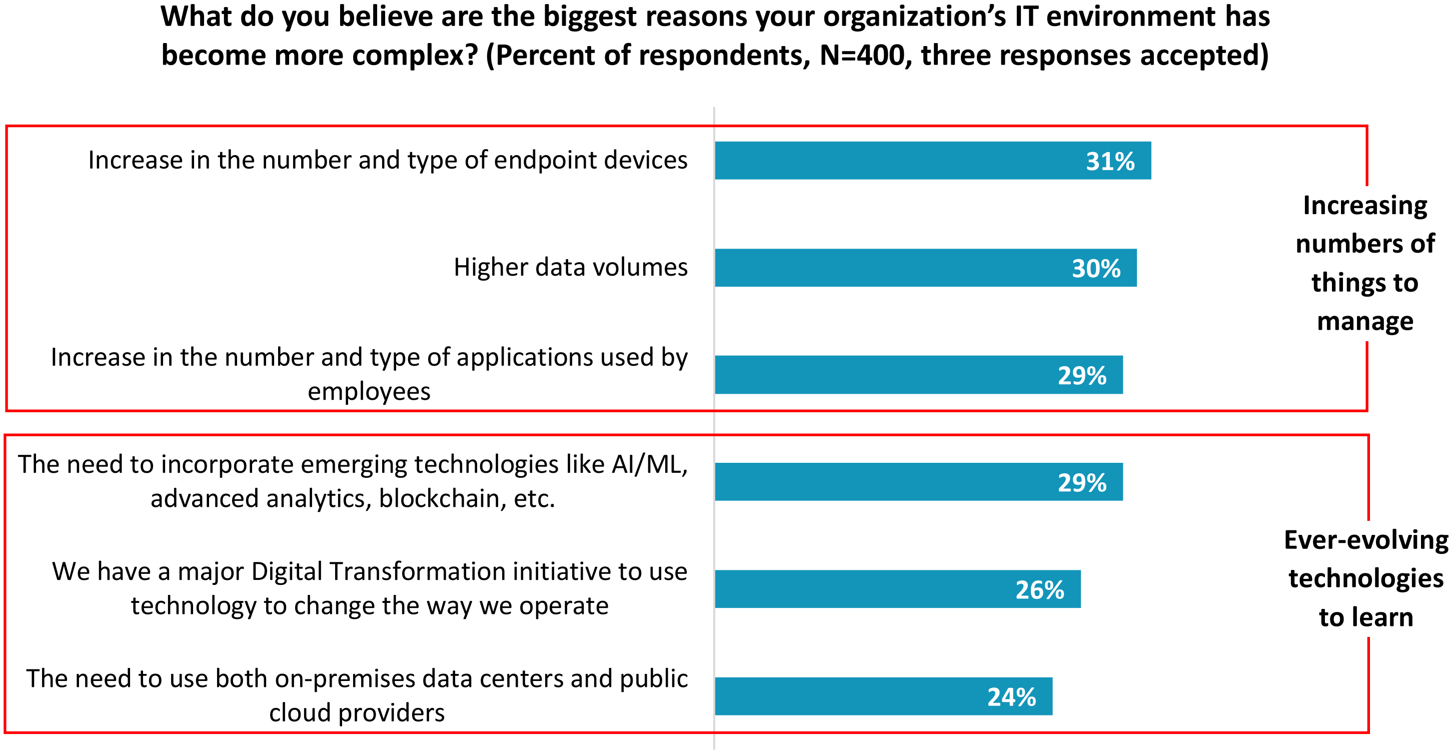
Elevated IT Complexity Fueling the Risk of Configuration Drift

Delivering effective and reliable IT services has always been a complex endeavor. In recent years, that complexity has ballooned. Recent ESG research shows that 66% of surveyed IT decision makers believe IT is more complex than it was just

[1] Source: ESG Master Survey Results, *2019 Technology Spending Intentions Survey*, March 2019. All ESG research references and charts in this solution showcase have been taken from this set of master survey results unless otherwise noted.

two years ago—not a long time for a business. When investigating the drivers of this increased complexity, (see Figure 1) two categories emerge, both of which create environments conducive to infrastructure configurations drifting away from their best practice ideals.

Figure 1. Top Six Factors Driving IT Complexity



Source: Enterprise Strategy Group

1. **An ever-increasing amount of stuff IT needs to manage.** A basic need to scale IT services with the business has existed as long as technology has been part of doing business. But now, the link between data leverage and positive business outcomes is accelerating the volume of things to manage. With more endpoints, more storage devices to support higher volumes of data, and more servers for the increased number of applications, the volume of architecture configurations that must be implemented, recorded, and maintained scales dramatically. This increase in IT components and complexity is rarely accompanied with an equivalent increase in personnel for support.

   This scale is happening across every deployment model. For example, while the growing adoption of public cloud services is capturing the attention of the IT press, 49% of IT organizations surveyed by ESG expect to increase their spending related to on-premises data storage infrastructure. The resulting volume of work on- and off-premises can often overwhelm IT admins, increasing the risk of mistakes while making shortcuts even more attractive.

   Unfortunately, IT cannot simply slow down the pace of deployment for necessary due diligence activities when demands spike. Modern businesses harshly judge IT when delays in service impact business opportunities, as 25% of business executives think IT is a business inhibitor. Slowing initiatives, even for the right reasons, can make IT an easy target for blame when a business misses its digital objectives. All of these factors exacerbate the risk of configuration drift events.

2. **The onslaught of new technology that IT must learn, integrate, deploy, and manage.** New technology is supposed to be IT's savior, offering innovations that address key pain points and free IT to work on more important endeavors. Research suggests that this is not necessarily the case: Yes, innovation is beneficial, but it has a cost. Understanding how each new technology impacts the application environment—and then adjusting the infrastructure design, architecture, and workload balance appropriately—takes time to master (time IT often does not have).

   Similar to the scale of IT, the introduction of unfamiliar innovation increases the volumes of configurations IT must implement and manage, increasing the risk of configuration errors and drift. Additionally, the integration of new applications and technologies requires new learnings. As a result, existing experience and training on former best practices and deployment configurations are not only less valuable, they increase the risk of configuration mistakes as admins, under pressure to keep pace with digital business demands, are tempted to guess at the right configuration rather than taking the time to learn the new best practice. And, in an ironic twist, IT may not be afforded the luxury of extra resources to learn a new technology because new technologies are often selected to help reduce the personnel necessary for infrastructure management.

Even for those firms that understand the need for increasing staff size, scaling personnel is a losing battle. Businesses are already hard-pressed to hire all the experts they need. For example, 38% of surveyed IT decision makers identified IT architecture and planning expertise as a top skill shortage, making it the second most commonly identified IT skill shortage, behind only cybersecurity.

With accelerated IT timelines and scarce personnel, shortcuts become attractive. Methodical, manual due-diligence activities become more a luxury than a common practice. As a result, an infrastructure design that was once optimized for efficiency based on best practices slowly morphs into something inefficient, insecure, and less robust. Additionally, without proper oversight tools, this slow transformation is often undetectable until an issue such as a breach or outage occurs.

What Is Configuration Drift?

The hidden, unpredictable nature of configuration drift makes it a complex issue to address. Business is a fluid process, full of ebbs and flows, and new workloads and infrastructure continuously need to be deployed. As a result, configuration drift is often a natural occurrence. When changes to software and hardware are made in an ad hoc fashion, not recorded, or not tracked in a comprehensive and systematic way, the state of the IT infrastructure drifts away from best practices.

Examples of configuration changes that can induce drift include untracked or erroneous changes to network addresses, firmware revisions, and updates to best practice configurations. These can be the result of malicious activities but are often simply the result of good intentions: A well-intentioned administrator might make a bad adjustment to remedy a current outage, take a measurement, or perform some type of "out of process" test on the infrastructure to save time.

Despite people's good intentions to remedy process breakdowns after the fact, another fire might start, or someone else could close the ticket before staff has free cycles to go back and do due diligence. Processes exist for a reason, but in the real world, the need for speedy service delivery or issue resolution can drive well-intentioned, smart personnel to skip steps.

Additionally, given the scale of modern IT infrastructure environments and the prevalence of element-level management tools that manage one device at a time, finding the few components that may be configured out of alignment becomes even more difficult.

As a result, configuration drift is an often-hidden issue, one difficult to detect without painstaking inspections. Over time, as configurations drift further away from best practices, multiple negative outcomes arise. Efficiency or performance may be reduced as bottlenecks appear or costly incidents may occur. Security gaps might emerge. Misconfigurations can even lead to partial or full outages of core IT services.

Addressing Configuration Drift

Technically, IT organizations should be maintaining detailed information about all configuration details, including all network addresses, software and firmware versions, and updates (including when each was applied).

Given the demand for speed and scale in modern IT, reliance on manual methods to accomplish those tasks will lose the battle. Additionally, the IT infrastructure environment is no longer limited to just the data center. The typical modern organization is dispersed. Multi-cloud, multi-petabyte environments are the norm, and the rise of the Internet of Things (IoT) is pushing the span of data systems to the edge.

Luckily, IT is not alone in the fight to address configuration drift. Multiple technology providers offer solutions. When working with an IT technology partner, here are some questions to ask to better understand their ability to help address this hidden threat:

- What tools does the vendor offer to automatically identify when configuration drift occurs?
- Do they make it easy to resolve drift issues when they occur? Is the resolution automatic or able to be automated?
- How much IT management overhead is involved in the resolution process?
- Assuming they offer tools for drift detection, are those tools able to supply information to the people who need to decide if the drifted configuration is the new norm? Blindly restoring the original configuration may reintroduce a problem that was solved by that configuration change.

Tools and automation that detect drift must be able to collect information that administrators can use to analyze the impact on both the infrastructure and the network and determine if it is desired or not. A collection of simple scripts running blindly is not enough. IT needs automation that can collect, analyze, and present information to the decision makers to decide how to deal with the drift.

What to look for when evaluating tools to help address configuration drift:

- The gathering of configuration information should take place through standardized mechanisms and interfaces. Often this is done through RESTful APIs.
- The format of the data returned must be standardized so that it can be exchanged and parsed with standard toolsets, such as JSON or XML.
- The configuration information collected and delivered must be meaningful, supporting actionable decision making. For example, data that states that an arbitrary value has gone from 3 to 8 is not useful, while data that states that a port has gone from disabled to enabled is useful and actionable.

If data centers were limited to only a handful of servers, configuration drift would not be an issue. But IT is more complex than ever before. Discuss the likelihood and impacts of configuration drift directly with your infrastructure partners. Incorporate suitable requirements into your regular technology evaluation criteria.

The Bigger Truth

Legacy infrastructure is never truly legacy. IT cannot simply “set and forget” the infrastructure they manage. In an era where data drives revenue and IT services open business opportunities, IT personnel are crucial to business growth. This link between IT and business success increases the value of the data stored across the company, while increasing the costs and risks associated with outages and security gaps.

Configuration drift is the perfect example of an issue that, in a perfect world, never rears its head. In smaller, more traditional IT organizations where processes can stay methodical, configuration drift is a far smaller issue. For modern businesses, on the other hand, “methodical” isn’t an option. The rest of the business is judging IT on both its resiliency and its speed of service delivery. In an effort to deliver the latter, the former can be neglected. To keep pace, modern, automated tools are necessary, ones that look for drift, detect it, and give administrators information to address it correctly. The measures by which IT is being judged have changed … so too should the rules by which IT judges its infrastructure technology.

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of The Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at 508.482.0188.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.