HOW IOT IS IMPACTING ITSM

Organizations are readily adopting digital technologies to support successful business operations. Connectivity is a key component of these technologies, allowing end users to access information from anywhere, anytime.

This connectivity is both an ITSM challenge and an opportunity. Connected devices can overwhelm IT's management of an evolving and rapidly scaling infrastructure environment. At the same time, the internet of things (IoT) can also assist and automate ITSM tasks such as incident management and service provisioning. Machines can communicate with other machines, systems, and mobile devices, with welcome results like automated processes and decreased burden on your workforce.

Let's explore the top five ways IoT impacts ITSM activities and strategies.

1. Expanding IoT big data cosmos

The challenge: Enterprises are adopting IoT rapidly, resulting in more connected devices, more generated data, and more end-points that require management. As data volumes skyrocket, device management complexity increases exponentially. IoT operations and the underlying ITSM capabilities become the primary bottleneck in adopting IoT-driven digital transformation. The quantity of incidents reported escalates, giving rise to false alarms, missed red-flags, and insightful patterns hidden deep in the IoT log metrics data.

The fix: ITSM frameworks adopted in the age of IoT and digital transformation must focus on data

quality over quantity, and the resulting issues of privacy, security, compliance, and infrastructure dependability. Doing data quality right will allow organizations to automate ITSM activities and decisions based on accurate real-world information. IT incidents are typically preceded by patterns of less sensitive glitches or anomalies. Advanced ITSM tools monitoring connected nodes and end-points can identify anomalous network behavior before the impact escalates and reaches end users.

2. Complex change management

The challenge: Configuring and controlling IoT devices is difficult in any digital transformation initiative. IoT technologies must operate in diverse, complex, and dynamic environments, yet device configurations must align with organizational policies around security and performance for every IoT application use case. Dependencies on proprietary standards and technology integrations contribute to limitations of possible configuration changes.

The fix: IT must maintain flexibility and usability of scalable IoT systems across a range of application use cases, without compromising organizational policies, security, and performance. Implementing the right ITSM frameworks and models helps manage and update IoT configuration changes accordingly. Advanced monitoring solutions to maintain visibility and control into vast IoT networks will be required to meet these goals. Relationships between IoT configuration items will be an integral component of effective ITSM strategies.

3. AIOps adoption on the rise

The challenge: Traditional ITSM incident management and response activities are rendered ineffective by the sheer scale of IoT big data, and manual processes cannot handle this complexity. More effective responses require visibility into the underlying processes, an accurate understanding of network performance, and the ability to respond proactively. AI for IT Operations (AIOps) has emerged as a viable solution.

AIOps can intelligently automate ITSM activities such as monitoring for the most impactful metrics, event correlation, and performance analysis. Predictive analytics can augment human intelligence and accelerate decision making. Without AIOps, IT spends significant manual resources (and introduces human error) on preventing incidents and promoting satisfactory end-user experience. AI is already seen as a requirement for ITSM to succeed in large-scale IoT network environments. However, AIOps is no silver bullet for the changing IT landscape driven by IoT.

The fix: Flexible frameworks such as DevOps must be adopted with a strategy in which AI is an enabler and active player for IoT-based digital transformation, not an afterthought for patching issues.

4. Monitoring and automation is reaching the edge

The challenge: Edge computing is on the rise, with Gartner labeling it a leading strategic technology trend. Rapid adoption of intelligent hardware IoT and introduction of high-speed 5G data transfer capabilities have brought automated ITSM decision-making and processes closer to the edge of IoT networks. The monitoring, diagnostics, and real-time optimization of performance, configurations, and security can take place at the network edge, relieving backend IT systems of data transfer, storage, and processing requirements. Additionally, the edge is a gateway to automatically implement ITSM processes specific to use cases. While all these are positives, don't forget that, as

with any new technology, implementation can be tricky. Deploying edge technologies can be hindered by a general lack of skills and support due to newness, the navigation of physical and cyber security, and essential cloud cost management struggles.

The fix: Have a plan in place that tackles both security and cost management situations. Harnessing low-cost tools for edge monitoring and support can help you take advantage of the transformation ITSM opportunities that IoT-enabled edge computing presents:

- Service delivery can be continuous, iterative, and automated.
- Configuration changes and incident and problem management can be prescribed and automated.
- Lower-level support needs can be delivered via self-service platforms instead of following a traditional manual service desk support cycle.

5. Rising ITSM spending

The challenge: Spending on ITSM efforts is increasing worldwide, and the impact is for companies to ensure they are spending wisely. Global ITSM spending is already on the rise, with growth expected to reach 9% CAGR by 2022. Global revenue for ITSM service and solution providers will increase by $2.65 billion between 2017 and 2022.

Another survey conducted among 400 IT executives and professionals worldwide found that digital transformation is driving an increase in ITSM spending. Of the respondents, 55% believe ITSM is "substantially growing in importance", and more than two-thirds of these organizations increased their ITSM budgets by at least 10%. (Only 12% maintained or reduced the budget for ITSM spending.) At the top of the ITSM agenda? The need for AIOps, driven by IoT technologies. Additional drivers for ITSM investment include improvement in IT operational efficiencies and long-term cost savings beyond IT.

The fix: Modern ITSM implementation is no longer limited to CapEx spending, but a strategic process to acquire improving ITSM capabilities, on a continuous and ongoing basis (OpEx). IT capabilities must encompass the people, processes, and technologies. Therefore, successful adoption of IoT-based digital transformation initiatives require dedicated budgeting to empower the workforce with advanced skills and technology solutions.