451 Research

Business Impact Brief

Innovations in Security Can Supplement IT Skills Shortage

The 451 Take

Digital transformation practices and the adoption of cloud delivery patterns have transformed IT. 451 Research constantly tracks technology trends at established organizations and newer ventures. Technology adoption continues to rise in all forms, whether on-premises or (increasingly) in cloud-based patterns, such as infrastructure as a service, platform as a service and software as a service.

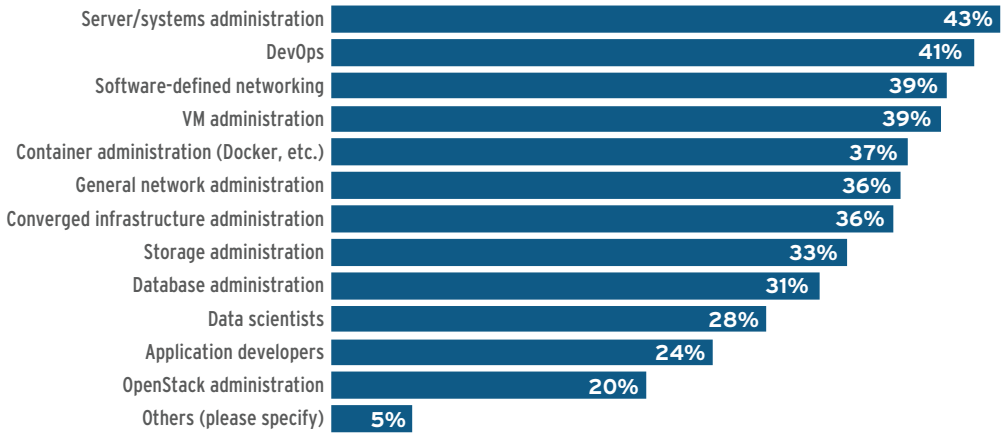
The quickening pace of adoption places significant burdens on development, security and operations teams. This is understandable because evolution to IT practices, such as DevOps and site reliability engineering (SRE) often require significant involvement and cultural change by the affected teams. In the meantime, increased demand, if left unmanaged, can result in negative business outcomes, such as outages or security incidents.

While the broad shortage of IT skills is recognized as a key issue, it is important to drill down to specifics. Infrastructure-focused roles are the most acutely impacted. The Voice of the Enterprise data below shows that there is a shortage of administration and networking skills spread across technologies. Still, baseline systems administration tasks – the mainstay of patching production systems, properly sizing workloads and managing users – are the ones most critically affected.

Skills Shortage in Operations

Source: 451 Research's Voice of the Enterprise: Servers and converged infrastructure, Organizational Dynamics 2018

Q: In which of the following areas does your organization currently face a skills shortage?



A lack of skills around broad systems administration practices is a key concern, with DevOps being a close second. Such skills are the foundation of many practices that may mitigate the overall volume of IT work, such as automated software patching and other tasks to maintain healthy and resilient systems.

Patching is often one of the more onerous and disruptive tasks for systems administration teams. Dubbed 'panic patching' for a reason, patching is often interrupt-driven – particularly for high-impact, high-urgency security-related patches, which may occur outside of normal schedules. The interconnectedness of systems and technology stacks often leads to patching having broad impact across the environment. Organizations have a powerful opportunity to rethink systems administration practices, bringing to bear the full spectrum of technology practices in a bid to optimize the delivery of IT services.

Business Impact Brief

Business Impact

AVOID GETTING STUCK WITH OLD THINKING AND PRACTICES. Organizations looking to improve quality of IT delivery using better or more efficient systems administration practices should frequently review and update their operational practices, considering new developments. This includes a combination of incremental improvements to existing processes and considering the use of more disruptive approaches to traditional IT issues.

UNDERSTAND THE ROLE OF RISK MANAGEMENT. Risk management is inherent in systems administration management, with operational risk evaluation embedded in every IT decision. In some cases, eliminating risk is the appropriate approach, and in other cases, shifting risk to other entities or to a different time when it can be handled better may be recommended.

LOOK AT ELIMINATING CLASSES OF ISSUES. Not all IT issues can be summarily eliminated. In certain instances, technology choices can simplify the environment and greatly reduce the burden on IT teams. Simplifications can arise from the automation of necessary tasks by applying modern practices, such as DevOps and SRE, or through thoroughly eliminating problems by rethinking commonly held assumptions.

CONSIDER EMBEDDED, NOT BOLTED-ON, SECURITY. One of the most interesting aspects of DevOps and SRE practices is the wholesale adoption of automation. In addition to general IT productivity benefits, this trend gives security teams an opportunity to embed a variety of security techniques into the infrastructure for intrinsic cyber resiliency with minimal impact to human workflows.

Looking Ahead

Moving forward, 451 expects organizations to continue digital transformation initiatives and technology adoption across on-premises and cloud delivery models. Systems administration and security teams must keep up. The increased adoption of more diverse computing options and more automated integration and deployment pipelines presents both a challenge and an opportunity. The potential for smarter practices is a key component for increased security and resilience.

Increased automation afforded by newer practices allows security teams to embed security into the IT infrastructure, and to explore newer approaches that can result in significant gains in time, skills and resources. One potential area worth exploring is the concept of moving target defense (MTD).

MTD refers to an approach, initially favored by the defense establishment, where the software environment can be automatically and seamlessly reconfigured to elude attackers. This can include a variety of techniques, such as system randomization, polymorphic binaries and scripts, dynamic compilation, and artificial diversity. These techniques aim to increase the cost and complexity of cyberattacks and work without the need for constant patching or updates. In particular, the intrinsic security of MTD can help reduce many of the burdens of patching.