



Anatomy of a Service Desk – Part 3 **“The Skeletal System”**



Mechdyne IT Services



While the individual pieces of infrastructure will be well-known to IT leaders – servers, firewalls, ISPs, telecom, etc. – the complexity and scope of the infrastructure required will be beyond many in-house support teams’ set-ups. IT teams look to managed service providers like Mechdyne to support end-users within specific service levels and relieve the human and technology capital required to set up a service desk that can provide timely and effective support to hundreds, thousands, or tens of thousands of end-users each month. The goal of this whitepaper is to outline some of the ways in which a professional service desk infrastructure goes beyond what is typically found within in-house support infrastructures.

Just as your bones act as your body's central support structure, the infrastructure of a service desk acts as the intricate framework and underlying support structure of a professional service desk. Much more than just an internet connection and a phone line, the service desk team relies on a variety of technology and hardware to remain effective.

Service Desk Infrastructure: The Key to Flexibility and Security

The underlying infrastructure of our bodies and a service desk enables both flexibility and security. Much like our bones protect our vital organs and our joints enable flexibility, a service desk’s infrastructure protects vital systems and client information and enables the flexibility to react to changing environments and client needs.

Flexibility within the Service Desk

“Flexibility” when discussing the service desk and its infrastructure means the ability to provide support in a changing environment. Much of this flexibility comes from built-in redundancy. A professional service desk needs to remain in operation during physical, environmental, and digital threats and challenges. While not an exhaustive list of the infrastructure required, the sections below outline critical pieces that enable flexibility.

Servers

Servers are critical to most IT processes, and this is no different for the operation of a service desk. A professional service desk may have more than 20 servers (physical and virtual) for normal operation and redundancy. These will be used for the Active Directory, Identity Management, and the critical Automatic Call Distribution (ACD) system.

Second Location

Depending on the organization’s uptime requirements and/or Service Level Agreements, a geographically different, but a mirrored site may be required. This is a critical piece to a Disaster Recovery (DR) Plan (*more on that later*). Just like backups, a second site can be accessed as needed with as little downtime as possible. For the DR plan to function properly, the two sites must be in sync at all times.

Business Continuity and Disaster Recovery Plans

Most (if not all) organizations require business continuity and disaster recovery (DR) plans. These plans enable the flexibility to continue operation during or after a major event by outlining the processes and procedures various teams need to take.

The business continuity and DR plans outline the redundancy the organization has created. This includes redundant technology, site(s), and people. If you own your own space, this can even mean having a redundant power source. While having redundant technology, site(s), and power are critical, people remain on the most important aspects of a DR plan. Gaps in responsibilities or skill sets can leave you vulnerable during a critical time. The plans should be validated at least annually, so the correct processes are in place to react to current threats.

Multiple Internet Connections

Internet connection redundancy is another critical point of redundancy. Multiple internet connections enable both clients and service desk technicians to access ITSM platforms or the ability to access the ACD system to field inbound contacts (chat, email, calls, voicemail, etc.) without interruptions.

Managing redundant internet providers is more complex than simply paying for 2 services. A professional service desk requires Border Gateway Protocol (BGP) integration and Cloud-based Domain Name System (DNS) providers to monitor the multiple paths and provide the most optimal path for end-user requests. These configurations also insulate the service desk from internet provider outages by automatically routing the internet traffic through alternate paths.

VoIP Gateways, SIP connections, PRI lines

End-users rely on the communication structure of the service desk to contact support and get back to work quickly. This structure includes:

- **VoIP gateways** - a networking device that converts a traditional (legacy) phone signal (analog or digital) into a (digitized) packet-based, Internet Protocol (IP) communication stream.
- **SIP connections** - Session Initiation Protocol (SIP) is a signaling protocol used for initiating, maintaining, and terminating communication sessions that include voice, video, and messaging applications.
- **PRI lines** - A PRI (Primary Rate Interface) line is a form of ISDN (Integrated Services Digital Network) line which is a telecommunication standard that enables traditional phone lines to carry voice, data, and video traffic, among others.



Phone calls are no longer the go-to contact method for many users. The service desk's infrastructure must include capabilities for supporting many different methods of communication.

Toll-free Service

While many in-house teams may not require toll-free phone numbers for the support team, externally managed service desks should provide this service. Again, this is more complex than at first glance.

The Mechdyne Difference

We manage the intricacies of offering toll-free service within our service desk while providing rapid, high availability without telecom carrier interruptions. We take our uptime commitments to our clients very seriously and have invested heavily in our telecom infrastructure. This infrastructure is comprised of

multiple tier 1 providers who have a global presence to eliminate single-point-of-failure at an inbound call entry point. This allows us to near instantaneously pivot between multiple last-mile carriers to deliver the call to our ACD system. This means that when your users call, they reach our support team.

A service desk's underlying infrastructure enables the flexibility to adapt to different situations, much like our own skeletal system. Instead of joints, service desks require redundancy in a variety of areas to react quickly and remain in operation.

Security within the Service Desk

Besides flexibility and mobility, our skeleton protects our internal organs. A service desk's infrastructure protects critical systems in a very similar manner. While your bones and a service desk's infrastructure are not the only security systems in place, they provide a critical layer of protection.

Good backups

Data breaches frequently bring organizations to a halt. Good backups protect from ransom demands for data and against loss of data in disaster scenarios. Not all backups are created equal, however. Air-gap backup solutions better protect against emerging cyber threats like ransomware because they are not located on the same network as the threat. Having the backups in a separate location can also reduce downtime from disaster scenarios.

Compliance

Certain industries have increased compliance and security requirements. Up to this point, the infrastructure discussed has been focused on securing the systems within an organization. When it comes to compliance, physical security is included in the discussion. Understanding who has access to data/servers and when they accessed them is critical. This can even include recordings of technicians doing the work, which may need to be retained for years in some cases.

Perimeter security with Firewalls which includes IPS and IDS capabilities

Intrusion detection systems (IDS) and intrusion prevention systems (IPS) are components of network security measures taken to detect and stop potential incidents. These capabilities are generally part of the next-generation firewalls (NGFW). As threats continue to evolve, this two-fold system is a critical part of the frontline security of the organization. Besides the actual firewall, organizations require people to monitor and remediate issues as they occur.

Internal or 3rd party Security Operations Center (SOC)

One of the ways organizations can effectively review, manage, and remediate the evolving threat landscape is through either an internal or 3rd party Security Operations Center (SOC). SOCs are also part of the team that helps organizations conform to their compliance standards, in many cases. Having a SOC in place (whether internal or 3rd party) decreases threat identification and reaction time allowing security response teams to effectively remediate threats quickly.

The infrastructure of a service desk acts in similar ways to the skeletal system of our bodies, promoting both flexibility and security for critical pieces. Without the critical processes and hardware outlined above a service desk will have difficulty “standing up” and supporting end-users across the organization. This is just one of the main systems that support and underpin a professional, managed service desk. We will examine the management team in the next and final installment of our whitepaper series, the “Anatomy of a Service Desk.”

About Mechdyne IT Services

Our 100% US-based IT professionals offer a full range of IT support services including an ITIL best-practices-driven service desk that enables end-users to get back to work quickly and improve the businesses for which they work. Mechdyne IT Services is a business unit of Mechdyne Corporation, a global technology leader creating distinctive electronic, software, and service solutions that enable discovery.

For more information, please visit mechdyne.com/it-and-audiovisual-services.