As the pace of change in technologies and the strategies to use them increases so rapidly, it is imperative for IT leaders to stop and evaluate the ideal “to be” state versus where they are today. Enterprises of all sizes, industries and geographies need to take a long, hard look at their capabilities and benchmark their skills and utility in several essential technology areas.

The Data and Network Maturity model in this paper describes the varying levels of adoption of the latest technologies and strategies in these four areas: **wired infrastructure, wireless, security and data center**. This helps both IT and business stakeholders understand how sophisticated their approach is—from fundamental to visionary—and illustrates what they need to do to move to the next level.

Organizations that utilize this maturity model will have a strategic leg up on their competitors because they will be able spot gaps faster, improve capabilities more easily and embrace a long-term vision for using information technology more effectively.
It is useful to think of this Data and Network Maturity Model as a series of stages, each utilizing increasingly sophisticated technology tools, processes and priorities. For instance:

**Stage 1: Fundamental.** These are the must-have, baseline requirements for each of the four technology pillars. In the Fundamental stage, organizations put in place foundation-level capabilities to help IT use data for essential—although probably not yet overly strategic—requirements. Organizations that don’t meet the technical and business requirements in the Fundamental stage certainly will struggle to survive, let alone succeed. But no truly successful organization will use data efficiently unless and until it progresses to the succeeding stages.

**Stage 2: Enhanced.** As pressures mount—competitive, regulatory, financial and others—organizations must quickly evolve their capabilities to fend off challenges and become better aligned with new market realities. This often translates into finding ways to reduce IT costs without impacting the ability to deliver essential services, or to safeguard the organization against risks such as cybertheft, compliance or data governance.

**Stage 3: Expert.** As the IT framework becomes a well-oiled machine and the organization strikes a balance between risk mitigation and service delivery, most organizations will look to seize opportunities to use data more aggressively and innovatively for better outcomes. In this phase, investments in technology tools and modernized processes are reflected in a bias for financial improvements, whether measured in sales increases, better profitability, faster ROI or market share gains. Additionally, steps taken in the Expert stage often are designed to address the cost or risk of not taking critical steps.

**Stage 4: Visionary.** Truly visionary companies don’t look for incremental gains. They are looking for breakthroughs that provide disproportionate, disruptive benefits that can be turned into sustainable competitive advantage. In the Visionary stage, the emphasis is on unearthing new tools and processes that often haven’t even been discovered or brought to market. Visionary organizations not only capture and analyze more data, but also are developing entirely new data types that provide unprecedented visibility into factors both inside and outside the organization.

**Applying the Data and Network Maturity Model to the Four Technology Pillars**

Truly innovative, successful organizations understand that using IT to its fullest capabilities means understanding this Data and Network Maturity Model within the context of the core technology pillars: wired infrastructure, wireless, security and data center. Here are some thoughts on this model’s applicability to each of those technologies, and how you can start planning to move to the next level of functionality and capability within each.
Remember that pretty much all the “cool” and exciting things happening in IT are made possible, or made better, by having a rock-solid wired infrastructure. BYOD, remote access, cloud computing, unified computing and more is enabled by secure, high-performance, reliable and scalable wired infrastructure.

**Fundamental:** Every organization now has basic LAN infrastructure—network adapters, routers, switches and the like. At the fundamental levels, this infrastructure is fairly static and delivers basic connectivity as required with computer-to-computer communications. At this stage, wired infrastructure has begun to support some type of wireless access, and there may be some—although not much—intelligence at the network’s edge. Server-based access control is enabled through Active Directory or some equivalent framework.

**Enhanced:** It’s increasingly likely that most organizations’ wired infrastructure has introduced redundancy/fault tolerance by now to enable seamless failover because of the essential nature of traffic over the wired LAN. Traffic is now getting heavier, both in terms of sheer volume and packet sizes since the networks are carrying more voice, video and other “thick media” types. Virtualized network infrastructure is likely to be an option here to reduce ongoing capital expenditures and to support the introduction of fabric services. Segmentation is taking place to prioritize and protect traffic, using such technologies as virtual LANs, Virtual Routing and Forwarding (VRF) and Multi-Protocol Label Switching (MLPS) over wide-area networks. The traditional focus on “feeds and speeds,” while certainly still important, now is giving way to resilience, fault tolerance and improved manageability.

**Expert:** As organizations’ data needs become more sophisticated, so must the physical network continue to evolve to support end-to-end services deployment. Autonomics—network self healing enabled by “machine learning” techniques—is a big step forward here, lessening the demands on IT staff for performance tuning and change management. This is likely to be an ideal setting for the introduction of software-defined networking, which abstracts networking software functions from physical network infrastructure, further reducing risk and improving agility. Of course, there’s a lot more emphasis on security at the network’s edge, not just at the core, in the form of more sophisticated network access control and authentication, as well as increased use of power redundancy techniques to ensure availability of physical network resources and services.

**Visionary:** Ultimately, taking wired infrastructure to the next level is less about technical advances (as important as they are) and more about smarter allocation of network resources and services to meet always-increasing user demand for bandwidth, speed, security and availability. Downtime becomes more than just expensive—it is extremely painful to all aspects of the business. Bandwidth is plentiful, so the focus switches to reducing risk and ensuring higher quality of service,
whether enabled privately or through a managed service arrangement. Over time, outsourcing some or all aspects of the wired infrastructure makes increasing sense due to the combination of essential uptime requirements that go beyond service-level agreements and achieve more than “five 9s” availability.

| WIRELESS |

Wireless is the rock star of today’s technology landscape, in large part because it enables so many important business trends including telework, always-on commerce, customer self service, audience engagement, employee empowerment and organizational agility. The Data and Network Maturity Model provides organizations with a schematic for going from wireless “table stakes” to the most sophisticated usage model.

Fundamental: Entry-level wireless can start with something as simple as a single access point, or even a small network of Wi-Fi antennas to blanket a relatively small area much like first-generation LANs did 30 years ago. Users can safely access the network through the Wi-Fi Protected Access (WPA) protocol, then moving to WPA2-AES, Lightweight Directory Access Protocol (LDAP) and remote authentication for centralized administration, improved data protection and tighter access control. Basic management functionality throughout the wireless LAN is baked in, and many networks will operate fine with tried-and-true wireless protocols such as 802.11a/b/g. Wireless capabilities typically are deployed and administered in-house, although many non-enterprise organizations that lack sufficient internal skills should consider some form of managed services to apply the correct policies to the WLAN.
and update configurations as needed to support the user community.

**Enhanced:** In order to ensure strong quality of service but also to improve reliability and safety, organizations should move to some kind of segmented service, such as wireless network access control for guest users. It’s also time to move up to faster Wi-Fi speeds, at least 802.11n and even 802.11ac for faster throughput, improved signal strength and increased security. Security is more important as more users request access to the wireless network, and as that network carries everything from intellectual property to customer privacy records. Bandwidth control also becomes more important here as more and more unstructured data—voice, video, social media and unified communications—becomes commonplace. Identity validation is increasingly valuable, both to enhance security and to avoid overprovisioning wireless infrastructure as more users attempt to move more data, access more applications and utilize more services over the WLAN. It’s likely that the organization will look for more automated WLAN management capabilities, and there are cloud-based options that can be “rented” or utilized in a managed services model that make sense.

**Expert:** To take advantage of increased wireless usage and optimized wireless applications and services, it’s now time to deploy a more dynamic, auto-adjusting infrastructure that intelligently dials up bandwidth and security in real time as conditions change. Here’s your opportunity to use your wireless network to make a real difference in how, when and where you conduct business.

Capabilities like secure roaming, enhanced bandwidth management, context-aware management and tighter integration with back-end wired infrastructure help organizations to leverage existing wireless investments and steer into users’ bias for wireless—and even virtualized—endpoints. In order to give users—as well as customers, suppliers and partners—the ability to do business 24/7 from any device and in any location, look for enhanced authentication in the form of 802.1x with directory service integration or EAP-TLS for certificate-based authentication. From a performance standpoint, you’ll need even faster transmissions in order to move bigger, more diverse data packets over wide areas, so you have to be using wave 2 802.11ac (or whatever the state of the art is at any given moment for wireless networking speed). In this phase, managed services partnerships become increasingly important as more technical, regulatory and applications knowledge is required, which translates into tight, symbiotic partnerships with third-party experts that have a long track record of success with wireless technology.

**Visionary:** Not that long ago, the things now considered commonplace in wireless networking were unimaginable for most. But the Data and Network Maturity Model, as applied to wireless, demands that organizations consider options
way, way outside the box. Faster networks, tighter security and nearly unlimited bandwidth are elements of every long-term wireless deployment and usage blueprint, which means that IT organizations must be looking around the corner more diligently than ever. Visionary IT staffs will not just watch the development of new performance, security and management standards, but also actively participate in them. Determining the right mix of on-premises and cloud-based infrastructure for wireless is critical to greater success over time, not just because the technology will continue to move at breakneck speed but also because understanding where the next intersection of business and IT will take place is harder than ever.

Software-driven policies must be created with the user’s need and perspective paramount, and those policies will need to be planned, deployed and managed throughout the enterprise. This must incorporate a wide range of public, private and hybrid cloud services. Over time, succeeding in the wireless segment becomes far less about faster transmission rates, more intelligent antennas or network bandwidth and much more about using software and dynamic policies to adapt to users’ needs, rather than the other way around. In order to become true visionary in the deployment and leveraging of wireless technology, organizations must partner with third parties that can help them imagine the previously unimaginable. More time and effort should be made by internal IT and business teams in identifying, evaluating, selecting and working with their wireless partners in order to turn wireless into a highly leveraged tool for business benefit.

**SECURITY**

The stakes have never been higher in information security, nor have the challenges to securing the enterprise been more daunting. Providing optimal security is a moving target, which makes the utilization of the Data and Network Maturity Model for security a mission-critical requirement.

**Fundamental:** Remember the days when security predominantly meant antivirus, intrusion detection, spyware and password management? Today, even fundamental levels of security are far more stringent because not only are cybercriminals more sophisticated than ever, but, security lapses can result in huge financial, operational, legal and regulatory problems. Today’s fundamental security defenses must be multi-layered, from the endpoint to the server, and from the cloud gateways to the applications and databases where critical data resides. Security must be layered into all infrastructure, with particular emphasis on securing the endpoints where so many attacks now occur. As threats proliferate, more emphasis needs to be placed on managing perimeter and core defenses from a single-pane-of-glass management console.

**Enhanced:** Security for mobile infrastructure, from wireless LANs to consumer-grade endpoints, must be a higher point of emphasis for organizations that need to protect their data. Not long ago, security for mobile devices meant simply being
able to lock down and wipe infected devices. Today, the emphasis is on software defenses, primarily enterprise mobility management to protect all possible points of entry onto the backbone network. Also, products like next-generation firewalls are being deployed with stronger protocols for data loss protection due to security breaches. Of course, when you talk about security, you also need to talk about its role in regulatory compliance, e-discovery and information governance. All of this requires a much higher, broader and deeper level of knowledge about security threats, from zero-day attacks and persistent threats to advanced targeted attacks, as well as techniques such as social engineering, spear phishing and “malvertising.” Trying to handle all of these requirements without sophisticated help from an experienced third party is a disaster waiting to happen.

**Expert:** Because security readiness is never “fixed,” organizations must be ready to move on a dime. Expert security defenses depend heavily on threat monitoring services, which have helped immeasurably in triangulating new threats based on their ability to mine huge amounts of data—something even robust in-house teams could never manage on their own. One of the key steps security and IT professionals need to take in order to become truly expert in defending the crown jewels is to change the mentality around security. For instance, it’s no longer just about building a moat around the kingdom. Instead, organizations need to also implement steps and layers, such as segmented networks and security around those layers, to create even more impediments to security threats. One thing to keep in mind is that more organizations are improving their security risk profile by working with third-party organizations. These organizations have been able to invest considerable time and money in state-of-the-art defenses, and to leverage their knowledge and insights on behalf of their clients.

**Visionary:** Although it’s becoming increasingly clear that cyberthreats are evolving every bit as rapidly as sophisticated new security defenses can be implemented, it’s also clear that an entirely new security philosophy is going to be necessary for most organizations. IT and security professionals, working closely with their business stakeholders and senior executives, need to consider defenses spanning a broad and growing spectrum of threat points. Just as securing the physical network quickly became insufficient when endpoint-based malware and intrusions became commonplace, new security frameworks need to account for all architectural models, including mobile, VMs and cloud. Security must be designed, implemented and managed on a 24/7 basis with overlapping tools and processes before, during and after attacks. Tools such as next-generation firewalls, enterprise mobility management, network access control and threat monitoring services must be used in concert with each other, but also with such practices as BYOD policies, identity management and even device decommissioning after employees leave the organization. For the truly visionary security professional, the watchwords are multilayered, eternal vigilance.
There may be no segment of the IT industry that has undergone greater change than the data center. Gone are those huge, monolithic rooms, replaced by smaller, flexible and dynamically changing computing environments. It’s important to think of data centers less as a “place” and more of a series of interconnected functions, often happening at multiple physical and virtual locations.

**Fundamental:** Today’s baseline for data centers is usually a single site, much smaller and less expensive to run than the data centers of just a decade ago, due to much higher-density servers, small-profile disk arrays and new data center power/cooling infrastructure designs, as well as the increased adoption of virtualized infrastructure. The on-premises data center typically is linked to a cold backup storage facility off site, either managed through a third-party hosting company or a cloud services provider.

**Enhanced:** Newer data center designs often are built around the concepts of redundancy, seamless failover and 100% fault tolerance. This often means established secondary—or more—data centers in remote locations to guard against unanticipated downtime sources such as cyberattacks and natural disasters. It’s fairly commonplace for data centers in this stage to include an outsourcing relationship for at least disaster recovery/business continuity, if not a fully managed data center environment. Virtualized servers and storage are typical, although they are not always managed cohesively.

**Expert:** As organizations increasingly adopt a multi-data center/multi-site architecture, the emphasis shifts to increased virtualization interplay among sites. Virtualized infrastructure in the data center—servers, storage and networking—is being managed cooperatively, with a strong emphasis on policy management and automation and a particular eye toward high availability and fast service delivery. The VM-based architecture is much more adaptive to change, reducing the onus on data center personnel and increasing their ability to work on transformative services and applications, rather than on keeping the lights on.

**Visionary:** The most forward-thinking organizations are going to move toward a software-defined data center (SDDC) model. With SDDC, total cost of ownership is reduced, management complexity is eased and business agility is increased. When all data center infrastructure resources are unified, pooled and abstracted, management can be centralized and easily orchestrated. Infrastructure components are configured and allocated as dynamic services for the users, as well as the applications running on the infrastructure. SDDC dramatically improves access control, policy management, security and bandwidth allocation. Again, visionary organizations are recognizing that the potential of SDDC is best exploited when working with a trusted advisor with an established track record for setting up and managing satellite data centers or even primary data center networks. This advisor handles far more than building out the data center itself; instead, this third party’s greatest value is in understanding how to align data center
design and management with long-term strategic business goals.

Summary
This Data and Network Maturity Model is designed to help both IT professionals and business leaders understand not only where they are in today’s use of technology, but even more importantly, what they need to do to avoid falling behind. Without a formal approach to assessing current capabilities in each of the fundamental technology pillars, organizations can find themselves at financial, operational, regulatory or reputational risk.

Using this model for technologies such as **wired infrastructure, wireless, security and data center** gives your organization a clear, actionable benchmark. This model enables organizations to plot a unique, clear and long-term course for business improvement, using technology from its most fundamental stage all the way to true visionary status.

Next Steps
Carousel Industries is your one source to help your organization create, navigate and benefit from the Data and Network Maturity Model. Carousel can help organizations move from whatever stage they are currently in for the four technology pillars to the stage they ultimately want to be in.

Carousel designs, implements and manages technology and cloud solutions that solve business problems and contribute to corporate growth. For over 20 years, Carousel has served the needs of a wide range of companies looking to maximize their use of their IT architecture, applications and data for quantifiable benefits.

Carousel provides a rich palette of technology solutions and services across the four pillars, as well as for voice, video, unified communications and cloud deployment. Deep technical expertise, combined with tight partnerships with the industry’s leading and most innovative technology providers, has allowed Carousel to help customers grow their businesses, solve problems and achieve competitive differentiation through creative and secure use of technology.

Visit [http://www.carouselindustries.com](http://www.carouselindustries.com) to learn more.