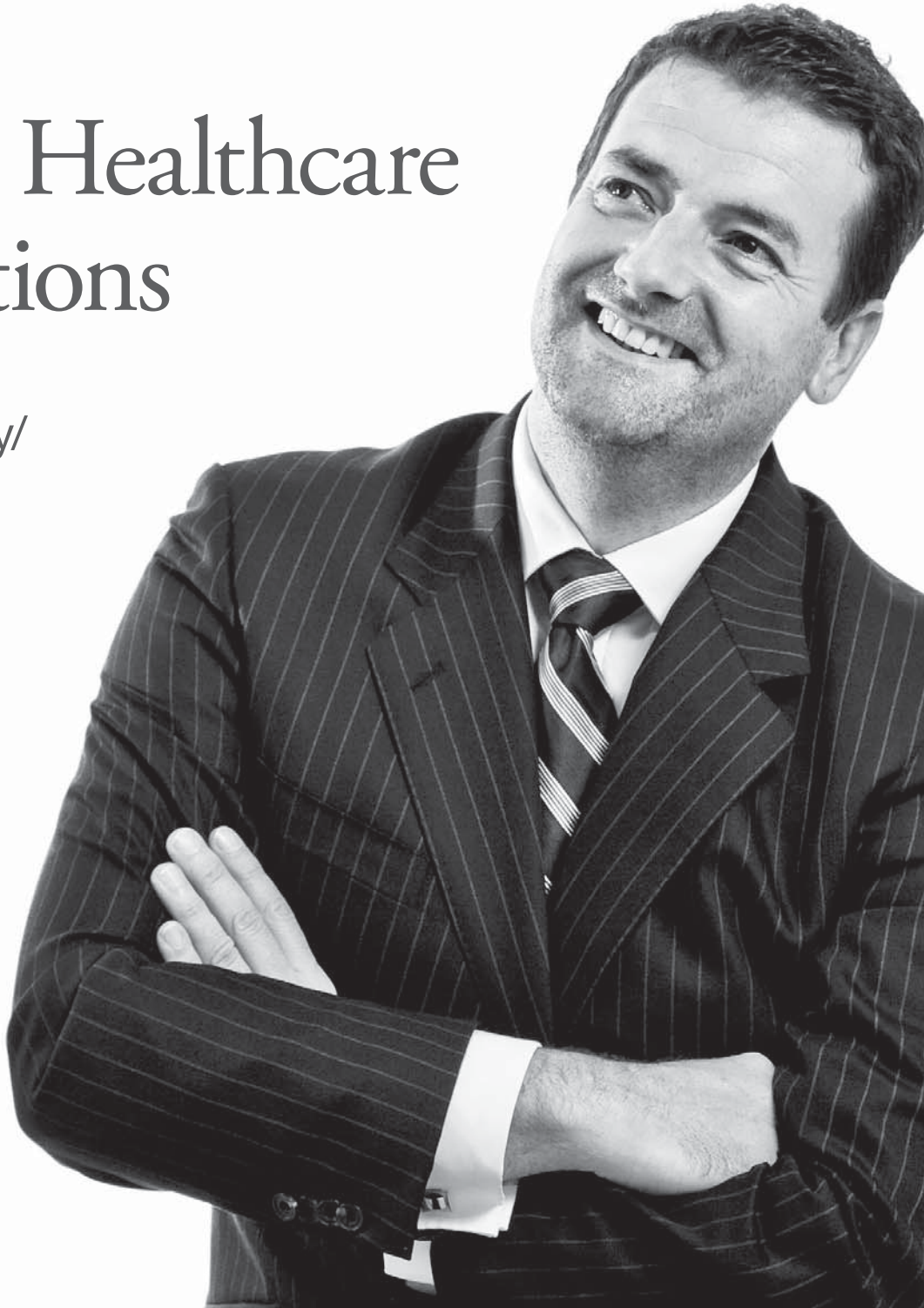
LOGICALIS
Business and technology working as one

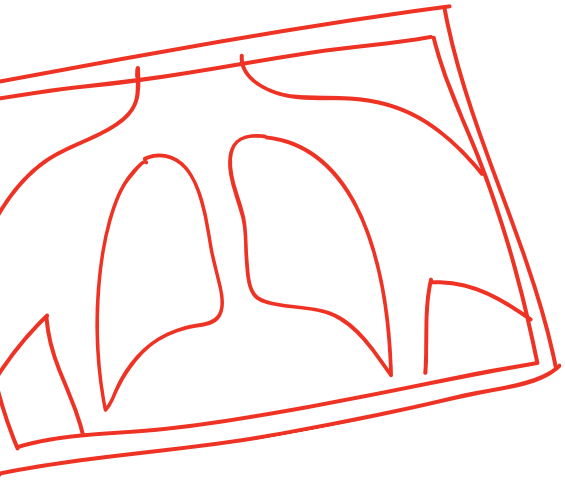
Triage for Healthcare Organizations

Business Continuity/ Disaster Recovery Planning



Triage for Healthcare

The concept of triage originated in World War I as a way to prioritize the treatment of patients on the battlefield.



A disciplined and objective process, the point of triage is not to identify patients with the most critical needs but to allocate services in a way that produces the best overall outcome during a crisis.

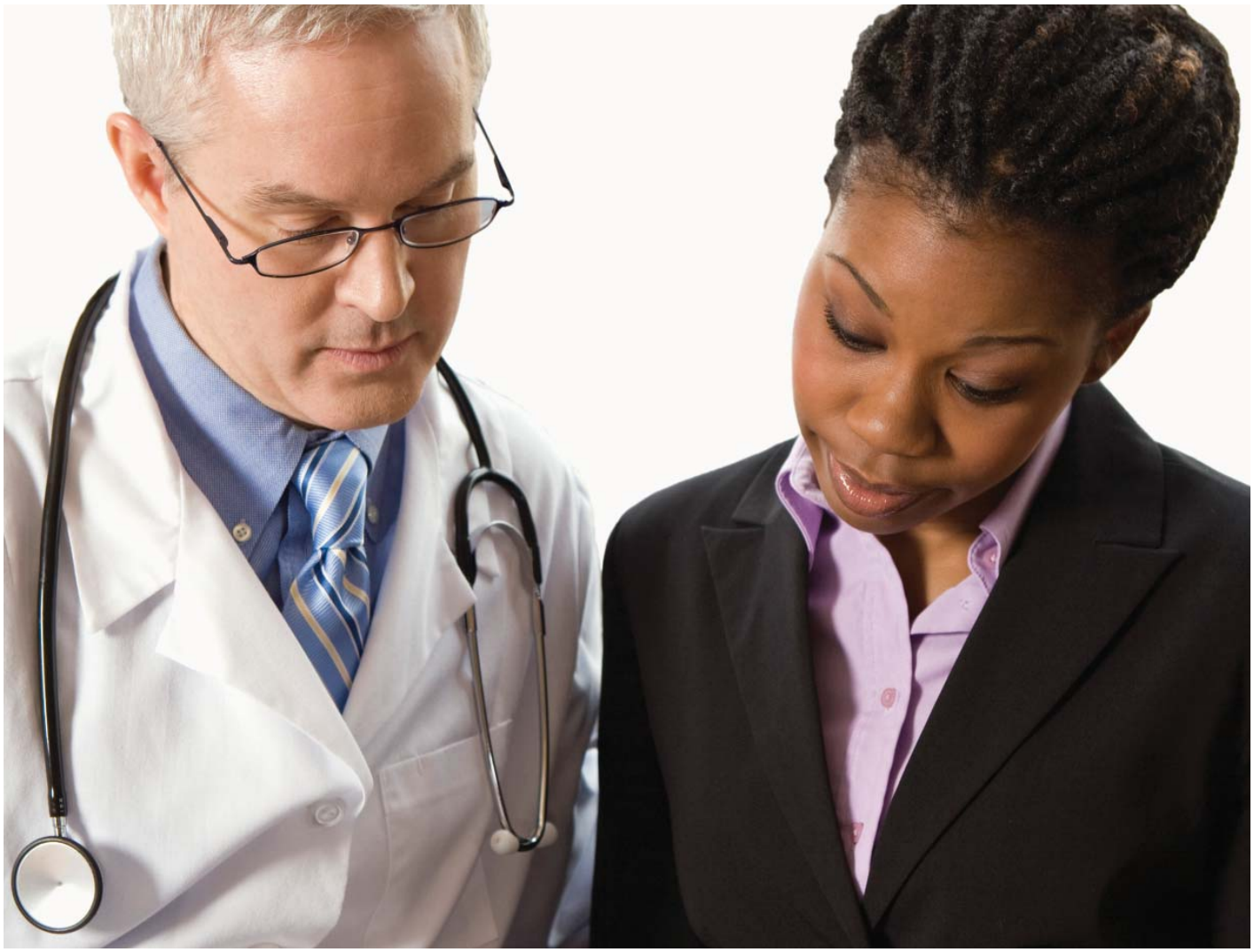
The healthcare industry today finds itself in a technology crisis. Healthcare IT departments were already scrambling to keep up with an exploding demand for technology in the delivery of medical services. That's before the federal mandate to provide electronic health records (EHR) tossed a time bomb into the paper records and photographic images that—for all of their shortcomings—at least provided hard copy backups for patient records.

And that's in addition to the ever-present risk of fires, floods, pandemics, computer viruses, reckless backhoe operators, lost/ stolen laptops, sabotage, bad luck and good old-fashioned, honest mistakes that occur in every industry.

Best Practices

Clearly some disciplined and objective process is required to evaluate the sustainability of the core clinical systems and business units encompassed by a healthcare IT environment to ensure the best outcome for the largest number of patients served by today's healthcare industry. That process is a best-practices approach to business continuity/ disaster recovery (BC/DR).

A strategic, phased approach to BC/DR systematically evaluates everything—technology, data, processes and people—that a healthcare organization depends on to function effectively and efficiently. A firm commitment to BC/DR will allow for the development of risk mitigation, continuous operations and recovery plans that can be implemented incrementally as budgets and resources allow.



A best-practices approach to BC/DR for healthcare organizations:

- Builds on actual data from within your organization
- Involves stakeholders across IT, clinical departments and business units
- Integrates and enhances what is already in place
- Establishes realistic benchmarks
- Adapts as you progress through the phases
- Ensures compliance with relevant regulatory agencies
- Articulates a comprehensive BC/DR strategy
- Keeps you in control at all times
- Provides peace of mind Beyond Disaster Recovery

Beyond Disaster Recovery

The uncomfortable truth is that focusing on disaster recovery in the data center is not enough. Disaster recovery needs to be addressed in the larger and longer-term context of business continuity.

In less time than most healthcare boards of directors have put off confronting their risk from some kind of data disaster, healthcare organizations' dependence on their IT infrastructure has become absolute. The recent economic recession increased IT dependence as organizations eliminated many manual processes, implemented IT-based productivity initiatives and cut IT budgets.

Further compounding the problem, mission-critical applications in healthcare are increasingly dependent on other applications in a web of interdependence that functions like a living nervous system.

"Although BC/DR is widely thought of as an IT responsibility, IT alone cannot ensure the effective functioning of a healthcare organization."

"In many healthcare environments today, practically the whole data center is required to be online to provide a relatively simple service to end users," observes Logicalis Solutions Architect Bill Mansfield. "The whole data center is starting to become interdependent down to the byte.

A healthcare organization's IT environment, business units and clinical departments need to work together interactively to address all of the needs of the patients they serve. Business continuity planning, as a result, requires that stakeholders from all departments share responsibility and accountability for the overall functioning of the organization.

Designed to Protect

BC/DR planning is not a one-time project. It is a living process like a healthy diet or an exercise routine. The scope of an effective BC/DR plan needs to be as broad as the organization it is designed to protect, ensuring that every detail is accounted for and all of the right stakeholders are involved. Most organizations have already conducted some level of business continuity planning. Many, however, have stopped short of making business continuity a way of organizational life.

This is admittedly a long journey. The first step is the development of a road map. Says Logicalis Professional Services Consultant Dan McMahan, "The business continuity road map lays out how you can get from where you are now to accomplishing your business continuity objectives. It identifies how you tie in each one of your platforms, as well as your asset management systems, and what options you have to out- or co-source the services required. The road map also projects a budget that you can take to the board of directors that shows specifically what needs to be done, over what period of time and how much it will cost."

Logicalis recommends a three-phased approach for a comprehensive plan. The three phases are:

Phase 1: Business Impact Analysis (BIA). This phase includes discovery, situation analysis, risk quantification/qualification, needs analysis and budgeting. A key deliverable of Phase 1 is a gap analysis report complete with data analysis and recommendations on risk mitigation.

Phase 2: Business Continuity Planning (BCP). This phase identifies strategic and tactical options and includes solution plotting, preprocurement, budget details and the creation of the BC/DR plan.

Phase 3: Business Continuity Program Development. This phase outlines technical development, procurement and initial implementation.

Each phase contributes data and policy improvements to the next phase in a process that reliably and predictably takes you toward your goal of sustainability.

Along the way organizations are evaluated progressively according to more than 50 criteria within five key best practice disciplines:

1. Continuous analysis
2. Risk mitigation
3. Contingency planning
4. Business continuance
5. Disaster management and emergency preparedness

Priorities

Determining the appropriate technology that will be required is often the easy part. An often more difficult challenge is negotiating internally what levels of risk different departments within an organization are willing to accept for their applications and data.

There are two key considerations to determine acceptable levels of disaster recovery:

1. Recovery Time Objective (RTO): How fast data must be recovered

2. Recovery Point Objective (RPO): How much data you can afford to lose

"Immediately" and "none," respectively, are the two most common answers from department heads.

When Logicalis' Mansfield asked one healthcare customer what would happen if the pharmacology application physicians use to order prescriptions online ever went down, his question was met by a look of disbelief. "This application can't go down," he was told. "It has to run."

Establishing appropriate, realistic and affordable RTO and RPO levels needs to be negotiated between the IT department, clinical departments and business leaders. It's often a balancing act. If the business is not willing to pay for the technology to eliminate interruptions, then the business has to pay the additional expense to develop, implement and train staff on downtime procedures (manual workarounds), which will be used as temporary stop-gap measures when automated processes are not available. Having an outside, unbiased business continuity planner present during such negotiations will help all stakeholders proceed to a mutually beneficial and acceptable conclusion.

Special Attention

Although the approach to BC/DR planning is essentially the same for any industry, there are areas of complexity—if not conflicting priorities— within healthcare that require special attention. Each area offers unique leverage points for negotiation.

For example:
Clinical imperatives: The highest level of authority in any healthcare organization belongs to the clinical departments and their respective doctors. Their decisions about the technology they want in their specialties rarely take into account what is needed to support it. That's one of the reasons Picture Archiving and Communications Systems (PACS) still exists in isolated silos in the data center. More physicians today, however, understand the benefits of an integrated IT environment that is accessible, interoperable and always available, and they see the advantages of participating in an effort that accomplishes those shared objectives. More hospitals are also realizing they need to provide integrated, interoperable services to attract and retain top physicians.

High levels of regulation: All industries have to comply with some level of regulation, but the extent and level of regulation in healthcare is unique.

Lots of agencies tell healthcare organizations what to do. The Healthcare Insurance Portability and Accountability Act of 1996 (HIPAA), for example, requires the privacy of a patient's electronic information and insists on a complete record of who looked at it and when during the whole period of time it has been stored—including where it could failover to or be replicated.

Other areas of interest for healthcare are the emergence of regional health information exchanges, the rapid evolution of cloud computing and the continual development of new technologies.

The Joint Commission, formerly the Joint Commission on Accreditation of Healthcare Organizations (JCAHO), a private sector, not-for- profit organization, has mandated that hospitals develop disaster management programs that include scalable models for community preparedness and 48 to 72 hours of standalone capability.

The American Recovery and Reinvestment Act of 2009 (ARRA) stipulates that EHR systems must be able to provide "meaningful use" of electronic patient records by 2015 or else healthcare organizations will not only forfeit stimulus funds but also be penalized through reductions in their Medicare and Medicaid payments. Needless to say, a central criterion for meaningful use is that the records are accessible whenever anyone needs them.

Many healthcare organizations have been cited for noncompliance by one agency or another for years. Chronic noncompliance not only reflects continuity risks, but it also contributes to the chronically high turnover of CIOs in healthcare. In virtually all cases, compliance with healthcare regulations is consistent with business continuity best practices. Being fully compliant may also stipulate audit trails and require completing the templates recognized by the specific regulatory agency.

Proprietary ISVs: Some large hospital information system vendors exercise a powerful influence over everything that goes in the healthcare IT environment. It's an influence they protect aggressively—even when there is no technological justification for their involvement. After years of being pushed around by the dominant independent software vendors (ISVs), however, more healthcare IT departments today are willing to assert themselves and implement technology that is driven by their priorities to serve patients instead of their ISVs' need to stay in control.

A major hospital complex in the Southeast, for example, was told by its ISV that it would not be acceptable for the hospital to implement its own remote business continuity site, proposing instead to outsource the hosting of its applications at several times the cost and a loss of local IT jobs. When the IT director presented the ISV with a design developed by Logicalis for the facility that would ensure no loss of data, ever, and no interruptions to applications of more than 15 minutes, the ISV acknowledged the design would work but insisted it would need to be the one to do the work. The IT director was not convinced, and the implementation of the Logicalis design is now in progress.

Organizations in all industries are confronted with similar changes. Healthcare has been slower to adopt technology, however, so the changes may seem to be occurring faster. A key part of the ongoing process of business continuity planning, as a result, is the ongoing evaluation of new BC/DR options as they become appropriate.

Key Considerations

Once realistic recovery objectives are identified, developing a tiered strategy that meets the specific requirements and budgetary constraints of your organization is relatively straightforward. Options abound for tier-one mission-critical applications that need some form of automated failover (short RTO). Less expensive technologies are available for applications that can be recovered more slowly (longer RTO).

Logicalis' Mansfield says there are two key aspects to business continuity from a technical point of view: high availability and continuous operations.

High availability means you can endure, or be reliant against, unexpected failures in your data center. There are several ways to provide high availability. "It is now possible to have high availability systems that are campus- and even metro-wide," Mansfield says. "If I lose services in my main building, the applications keep running in another building with no loss of application availability."

Continuous operations means you can endure, or be reliant against, planned or expected events—such as upgrades, maintenance and service—that need to occur without interruption of service. This level of protection is harder to accomplish.

Further Reading

Visit
www.us.logicalis.com/ms

Read
Logicalis feature article
"Efficiency on Demand"
www.us.logicalis.com/ms

"Providing continuous operations requires a deep understanding of how applications fit together," Mansfield says. A full dependency map needs to identify all of the elements—hardware and software—that form the complex web of technology required to provide services to a user. Once you have identified all of the interdependencies, Mansfield says, it's a case-by-case process to provide whatever level of both kinds of availability is deemed necessary. Projects identified by the evaluation process could include everything from revising change management procedures and implementing virtualization and replication to improving backup systems.

Choices

The key deliverables that result from a comprehensive BC/DR plan are choices. You get to decide what to do before a disaster instead of afterward or, worse, in the middle of one

Better yet, you get to choose what steps you and your CFO are willing to take to reduce or eliminate risks to your organization's business continuity. Having the knowledge gives you the power to act. A solid, tested BC/DR plan will allow you to be proactive, not reactive.

The completion of a BC/DR plan, for example, gave the board of directors of a major Midwest hospital complex the information it needed to make a commitment to spend the money to develop two data centers that are the mirror image of each other to ensure the continuous availability of its state-of-the-art integrated IT environment.

A pioneer in EHR, this hospital had transformed its data center from a decentralized infrastructure that primarily served billing and administration into a centralized system that accommodates the hospital's full scope of needs, including one of the most advanced EHR capabilities in the healthcare industry.

The whole infrastructure was developed with patient care in mind. From one pane of glass, a physician can pull up a complete patient profile, including billing, insurance, X-rays, lab tests—basically everything that is known about the patient.

A showcase of EHR in an integrated IT environment, this hospital's business continuity plan made it clear to the board of directors that it needed to invest in full synchronous replication at a second data center to ensure continuous availability of services.

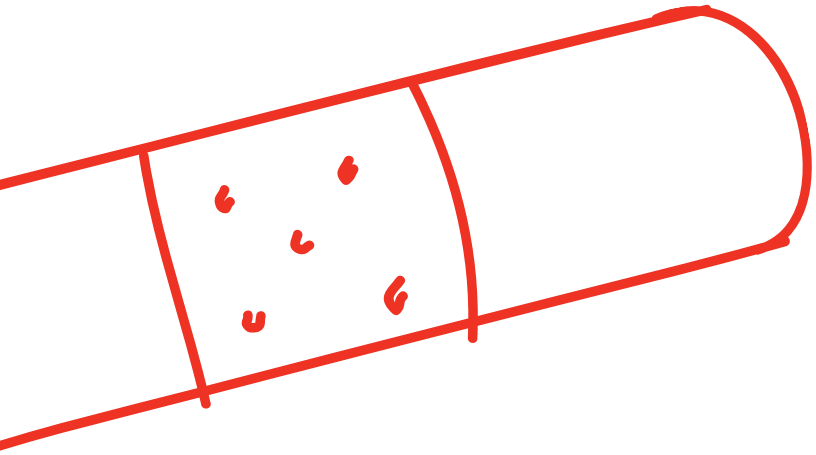
In this case, BC/DR planning helped all of the stakeholders collaborate on an integrated system that met all of their priorities. Besides facilitating the care of patients, the IT environment is equally responsive to the hospital's business needs. Like businesses in other verticals, hospitals frequently grow by acquiring other hospitals; the ability to easily integrate an acquired organization's IT can mean the success or failure of an acquisition. The IT department also benefits from having an integrated system, which means there is one place to look for everything.

Confidence

A typical BC/DR plan for a healthcare organization addresses key technologies, such as data replication for availability, server virtualization for rapid restart and IP telephony for integrated communications in the event of a threat to the effective functioning of the IT environment.

The true value of business continuity planning is not limited to technology. Done correctly, the exercise of developing and implementing a thorough business continuity plan opens ongoing conversations between IT, clinical departments and business units, which contributes to a sense of trust as well as a shared confidence in their combined abilities to work together as an efficient team for the greater good of the patients they serve.

This hospital IT environment is one of the first to be able to demonstrate "meaningful use" as required by ARRA for EHR. There are people at this complex who never use a pencil and paper.



What can we do for your organization?

Contact Logicalis to learn how we can help.

Visit
www.us.logicalis.com

Call
866.456.4422

About Logicalis

Logicalis is an international provider of integrated information and communications technology (ICT) solutions and services founded on a superior breadth of knowledge and expertise in communications and collaboration, data center, and professional and managed services.

Logicalis Group employs over 1,900 people worldwide, including highly trained service specialists who design, specify, deploy and manage complex ICT infrastructures to meet the needs of over 5,000 corporate and public sector customers. To achieve this, Logicalis maintains strong partnerships with technology leaders such as Cisco, HP, IBM and Microsoft.

The Logicalis Group has annualized revenues of $1 billion, from operations in the UK, US, Germany, South America and Asia Pacific, and is fast establishing itself as one of the leading IT and Communications solution integrators, specializing in the areas of advanced technologies and services.

The Logicalis Group is a division of Datatec Limited, listed on the Johannesburg and London AIM Stock Exchanges, with revenues in excess of $4 billion.