Design for digital

A business vision to prepare communications service providers for the cognitive era

Get started

6. Transformational opportunities and challenges

6.1 Your cognitive future

Data is the new natural resource. Yet 80 percent of data — the unstructured data that encodes language — is largely invisible to computers and has therefore been useless to us.

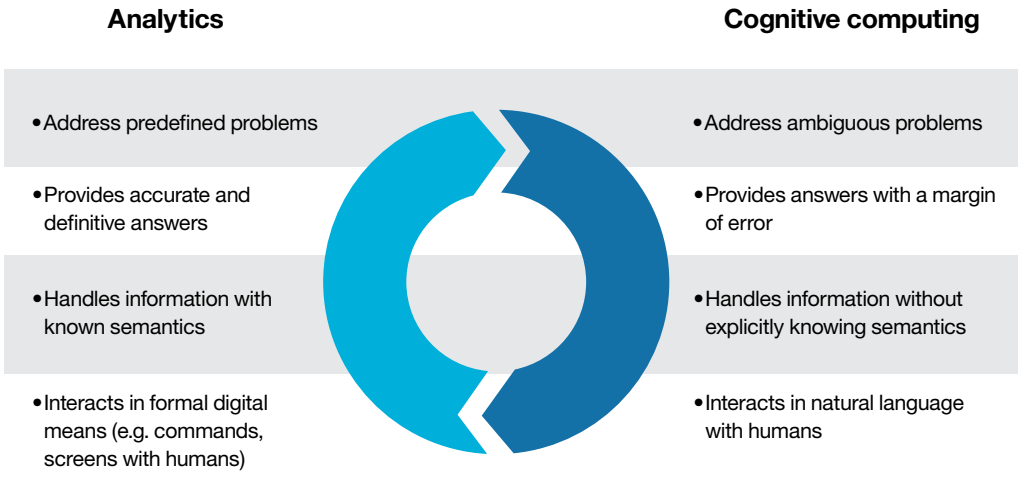
But IBM Watson applies cognitive technologies to help change how we approach and understand this information. It can ingest this unstructured data and not only understand it, but also reason about it, combine it with structured data and learn from it. Now, products, services and processes can, in a sense, think.

Welcome to the age of cognitive computing, where intelligent machines simulate human brain capabilities to help solve society's most vexing problems. For the communications industry, cognitive computing has indeed arrived, and its potential to transform the industry is enormous.

In the world of ICT, there is often talk of "the next big thing." Today many of these conversations are broadening, as cognitive computing is touted as revolutionary for ICT, many industries and, indeed, society in general.

For the communications industry in particular, the timing for this game changer couldn't been better. The industry has been facing a broad range of unprecedented disrupted forces, including evolving customer expectations, growing competition from non-traditional players, explosive growth of video traffic, rising cost pressure and increasingly sophisticated privacy and security threats.

Cognitive computing complements traditional analytics by creating a value continuum for the industry.



At the same time, CSPs have to manage massively increasing volumes of data, from a wider range of sources, brimming with latent insights that could potentially redress some of these issues. Unfortunately, they are unable to unlock the full value of the data at their disposal. As the potential for insight increases with additional data, so, too, does the challenge in managing this data.

Advances in cognitive computing can help CSPs manage this increasing volume of data while exploiting it for greater insights. Cognitive-based systems can build knowledge, understand natural language and provide confidence-weighted responses. And they can quickly locate the proverbial needle in a haystack, identifying new patterns and insights—something particularly relevant for activities in the fast-changing communications industry. Indeed, cognitive capabilities could help CSPs optimize value from data already within their reach, giving them a leg up on new market entrants that don't have access to the same data.

Our research indicates that communications industry leaders are poised to embrace this ground-breaking technology and invest in cognitive capabilities to spark a renaissance in the industry. Indeed, 85 percent of executives familiar with cognitive computing believe it will play a disruptive role in the communications industry.

Some leading CSPs are beginning to develop use cases for cognitive computing. Examples include answering customers' questions, supporting call centre agents and retail store associates, improving predictive network maintenance via machine learning, and analyzing people related trends such as skills and employee engagement. Furthermore, CSPs could develop new revenue streams by using cognitive computing to offer new services to businesses in areas as diverse as healthcare, banking, insurance and smarter cities.

6.2 Cloud for Telecommunications

Our experience with cloud computing underscores its power to fundamentally shift competitive landscapes by providing a new platform for creating and delivering business value.[1] To take advantage of cloud's potential to transform internal operations, customer relationships and industry value chains, organizations across industries must determine how best to employ cloud-enabled business models to drive sustained competitive advantage.

CSPs have a unique opportunity to capitalize on cloud computing, both as providers and users. As providers, they are the backbone of cloud technologies, helping all other industries translate capital expense into operational expense, reducing total cost of ownership and enhancing performance. With cloud, CSPs can radically change their positioning in the value chain and create new monetization avenues as digital service providers offering enterprise and consumer cloud-based services.

As users of cloud technology, CSPs can transform internal IT and data center operations. Moreover, the industry is transitioning to cloud-based networking, in which functions previously delivered as appliances are delivered as software components running on a cloud infrastructure. The emergence of software defined networking (SDN) and network function virtualization (NFV) is crucial for CSPs, enabling significant cost take-out, greater agility and faster time-to-market.

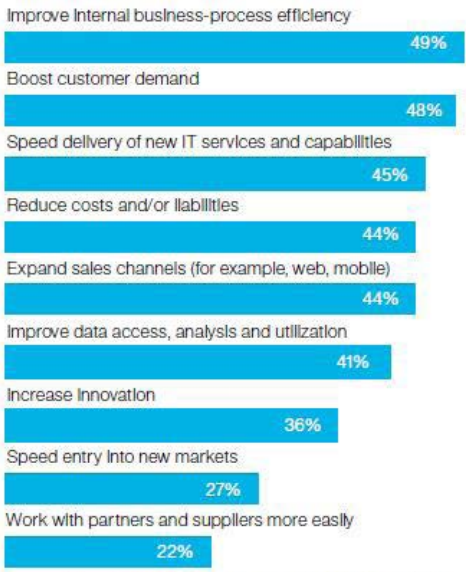
Cloud is transforming the business of telecom

For the telecom industry, cloud computing offers the potential for significant improvements. Cloud can help CSPs create new businesses, redefine customer relationships, transform and optimize operations, and expand business agility and capability.

Leading CSPs leverage cloud for:

- Operational innovation – Simpler and faster processes drive internal efficiency; reduced complexity enables better governance and expanded access to more and broader data to manage risk; and IT capacity is better aligned to business volumes.
- Revenue model innovation – Customer relationships, data and other assets are monetized more readily; time-to-market is enhanced; and relevant partner services are incorporated more easily.
- Business model innovation – Third-party services extend into the telecom ecosystem; open collaboration and sharing are expanded; new types of business can be pursued; and innovation is introduced systematically.

Clients have realized significant benefits as a result of cloud adoption during the last two years



Source: "Mapping the cloud maturity curve" by EIU, March 2015.
Question: "What business benefits has your company realized as a result of using cloud technologies?" n=100

As part of the "Mapping the cloud maturity curve" survey by the Economist Intelligence Unit (EIU) in March 2015, 100 CSP executives were asked to identify their organizations' top business drivers behind cloud adoption. The top-three drivers cited were to improve data access, analysis and utilization (cited by 43 percent); expand sales channels (36 percent); and boost customer demand (36 percent).

In addition to seeking the motivations behind cloud adoption, the survey also asked telecom executives which benefits their organizations have realized as a result of cloud. Forty-nine percent of the same industry executives said cloud has improved internal business-process efficiency, while 48 percent indicated that it boosted customer demand, followed by 45 percent who said it sped delivery of new IT services and capabilities.

As cloud adoption by CSPs matures, other benefits will also accrue. CSPs and their customers will be able to design, prototype and deploy applications quickly. Organizations will benefit from new user-driven, mobile and cloud-centric information technology. Cloud will support transformation of enterprise IT functions, roles and responsibilities. And business managers will increasingly use cloud for application development to enhance agility.

Along with benefits for the enterprise, cloud brings increased customer benefits. Cloud can facilitate new and expanded channels, as well as improve access to client data, allowing for better tailored products and services. Cloud also enables CSPs to transform and redefine how people consume video. By fostering more integrated, compelling customer experiences, cloud helps strengthen customer loyalty.

To succeed with cloud, CSPs have to assess its impact on the operating model and determine what actions are required.

- **Source and manage partnerships and alliances efficiently.** Automate procurement and sourcing functions. Define service-level agreements to secure customer data in a shared environment.
- **Proactively redesign business architecture and processes.** Integrate legacy processes into new cloud-enabled, dynamic processes. Establish available and reliable cloud-based platforms.
- **Change organizational design and governance.** Prepare to mitigate data privacy and compliance risks with strong risk management systems.
- **Evaluate existing performance management.** Develop strategy and metrics that address new levels of reporting complexity. Build performance metrics into contracts for cloud-based services.
- **Develop critical new cloud capabilities.** Foster skills in customer and service orientation; virtualization and network technologies; and relationship management. Build deeper analytic and operational capabilities.
- **Increase adoption of emerging technologies.** Update IT strategy to support new business strategy and cloud enablement. Adjust budgets to cover costs of legacy systems and new network bandwidth.
- **Reassess location strategies for optimal cloud adoption and to enhance the customer experience.** Decommission or consolidate technology assets.
- **Promote organizational culture changes.** Educate employees about organizational changes, addressing resistance by IT and other functions.

IBM Cloud is designed for the enterprise and is well suited for the emerging hybrid cloud era – an era that is already upon us, with Garner predicting that nearly half of large enterprises will have hybrid cloud deployments by the end of 2017.

By seamlessly marrying a company's systems of record with new and emerging systems of engagement, IBM can help clients mine data as the new natural resource while protecting privacy and security; quickly integrate existing and new services and data to drive new innovations; and easily control, manage and secure where data and apps reside.

With SoftLayer as the foundation for IBM's expansive cloud portfolio, IBM has announced numerous acquisitions in this area, including in 2015: Gravitant, StrongLoop, Cleversafe, Compose, and Blue Box.

IBM launched the Bluemix cloud computing platform with a $1 billion investment in 2014, and since then it has grown rapidly to become the largest Cloud Foundry deployment in the world. The open-standards-based Bluemix catalog includes over 120 tools and services spanning categories of big data, mobile, Watson, analytics, integration, DevOps, security and Internet of Things.

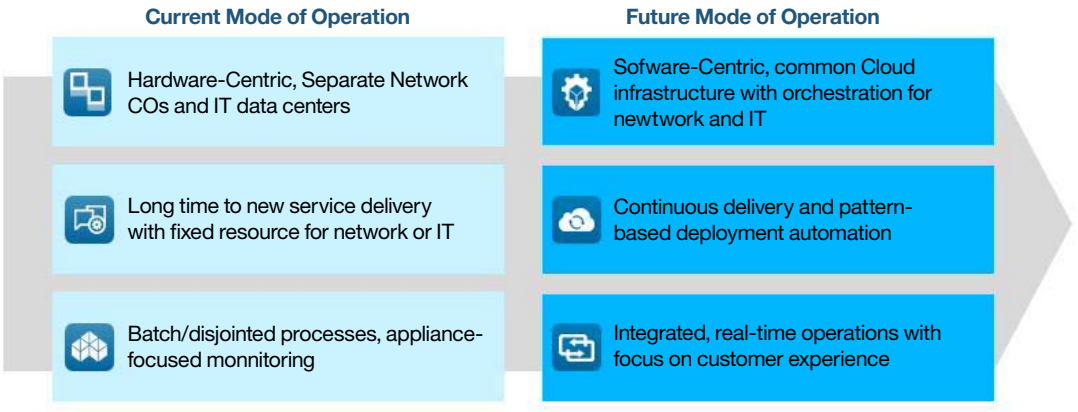
6.3 Network-related challenges

6.3.1 Transition

The industry is in the midst of a transition to software based networking, where functions that were previously delivered as appliances will in future be delivered as software components running on a cloud infrastructure. The emergence of software defined networks (SDN), network function virtualisation (NFV) and cloud radio access network (C-RAN) demonstrate that we are now in the middle of this transition. Infonetics forecasts that the carrier SDN and NFV market will reach $11 billion by 2018.

The speed of the transition will challenge many operators. We believe that the transition will be consolidated into a matured trend by 2020, and while this matches the timescale for 5G, cloud based networking applies equally well to fixed networks and earlier mobile technologies.

The transition to cloud based networking will disrupt the existing industry supply chains, as new vendors emerge to create virtual network functions, and in parallel to provide the required cloud infrastructure. Existing vendors will need to consider whether to continue their current product strategies or to adapt.



Today, networks are built using standard components defined in industry groups such as 3GPP (SMS-SC, HSS etc.). The transition to cloud based networking will see a period of innovation as vendors implement new virtual network functions. This will require operators to take end-to-end responsibility for the architecture of the network, going beyond vendor selection for well-defined network elements.

In addition, during this transition period operators will face a new challenge: how to assemble a complex set of virtual network functions (VNFs) into a network. We believe that this will give rise to a new role in the CSP ecosystem — the network system integrator. Not all operators will have in-house skills to integrate and test a complex set of VNFs from multiple vendors. They can choose to outsource the entire process to a single vendor, as often happens in emerging markets. An alternative is to engage a systems integrator, who will take the prime responsibility for delivering a working solution. Some tier 1 operators may choose to perform this role in-house. In all cases a key decision is around governance and the retained design authority.

The skills required to design, deploy and operate a cloud based network will affect all operators. New skills such as cloud, SDN, NFV will be needed across different parts of the operator such as design and operations. These skills are not widespread and require an understanding of distributed software and cloud in addition to telecommunications.

The operations (tools, process and technology) will need to transform from reactive to real-time in order to deal with a network that can be enabled in real time. This will then require the development of predictive capabilities. In future it will also bring about the need for cognitive operations. We illustrate this trend in the diagram below.

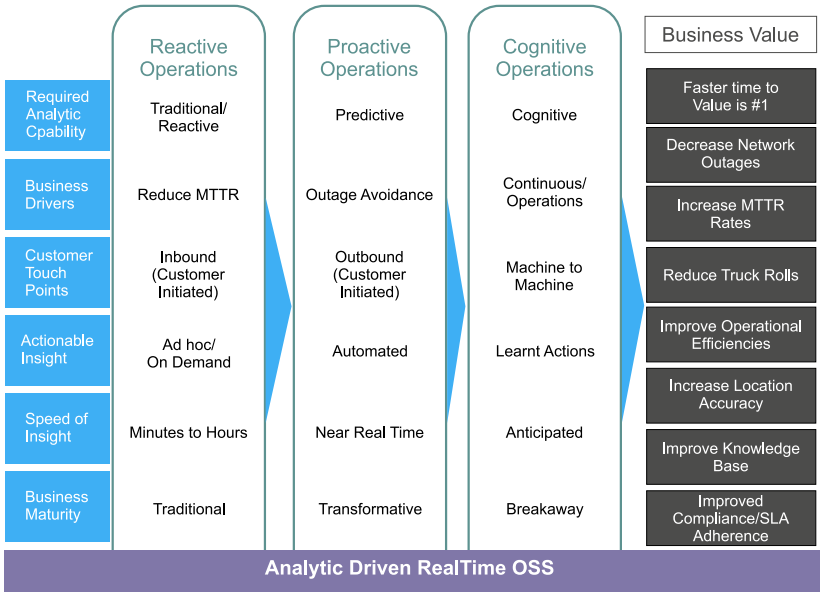
The changes will also put pressure on billing and mediation systems to adapt quickly to new offerings and capabilities that come from outside the telecommunications industry.

6.3.2 Benefits and design aspects of full cloud networking adoption

The implementation of a next generation cloud based network can lead to the following quantitative benefits, only in the network domain:

- Capital expenditures reduced and return on assets improved by up to 30-50%
- Network capacity and performance improved by 50%
- Monetization of the network platform
- Improving time to market of new network based capabilities and capacity by several orders of magnitude

To achieve time to market improvements, the future Digital Service Provider will need to complement the ‘cloudification’ of the network with other capabilities like Agile Network DevOps (see section 7.3.1)



Cloud based network and the Internet of Things

The flexibility of cloud based networks means that operators can adopt new product and service strategies. An operator may choose to deploy multiple virtual IEPCs to enable Internet of Things business units, where different customers (utility meter, automotive) have entirely separate infrastructure.

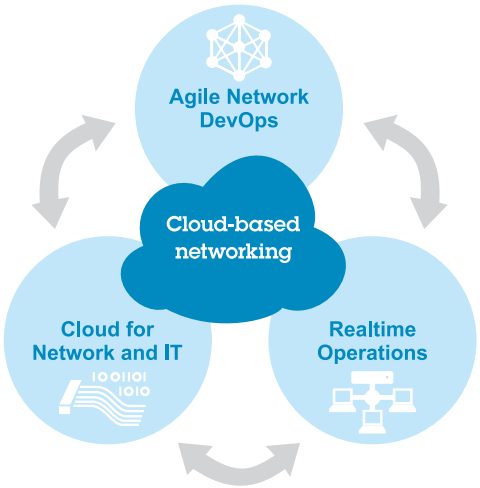
Design aspects

The assumption of a cloud infrastructure as a fundamental base to implement a new "All-IP" network requires operators to consider different approaches in the design of cloud networking:

- How many cloud data centres are required to deliver all the service? There are arguments for centralization to a small number of cloud centres in a country; equally there are arguments for distribution, and moving capabilities to the edge of the network. Both models are currently being explored by operators around the world.
- Implementing a cloud based network requires the ability to deploy a complex set of virtual network functions which are interconnected by a complex virtual network. Cloud orchestration enables this deployment to be completely automated, according to a set of templates defining the topology. Orchestration, and its interaction with the existing Operational Support Systems, is a key enabler for operators.
- Much cloud technology is being developed in the open source community, for instance Linux, OpenStack and CloudFoundry. Operators will need to understand how these communities work, and also the governance processes around taking products from the community and deploying into production.
- Telecommunications networks are critical national infrastructure and require a high degree of security and integrity. Cloud based networking does not change the underlying security requirements, but does require reconsidering how they are achieved. The implementation of cloud based networking changes the security threat model, since the underlying cloud infrastructure is now a very attractive target. Again skilled staff, revised design principles, and strong governance will be essential to securing the new infrastructure.

A case study on cloud networking of the future implemented today for…IBM.
IBM operates 7.4M square feet of infrastructure for global enterprises in over 430 data centres. One common scenario is provisioning a web server cluster, load balancer, firewall, and virtual network. Our data indicates that provisioning computer infrastructure usually takes less than one day. In contrast, processing the network and appliance service requests takes 6-10 days on average, and is dominated by the complexity of network configuration and firewall rules. The automation of network functions using SDN has the potential to reduce the elapsed time to hours.

Deployment of a virtual network function in production will involve multiple sets of virtual machine images each deployed in multiple virtual machines (e.g. load balancers, CSCFs, HSS servers and database servers in a virtual IMS). Configuring a complex cluster of virtual machines without automation is slow and error-prone. Templates, which define both the configuration of the individual virtual machine images and the connectivity between virtual machines, are essential components of a network automation strategy. The IBM Cloud Orchestrator supports HEAT and TOSCA templates.

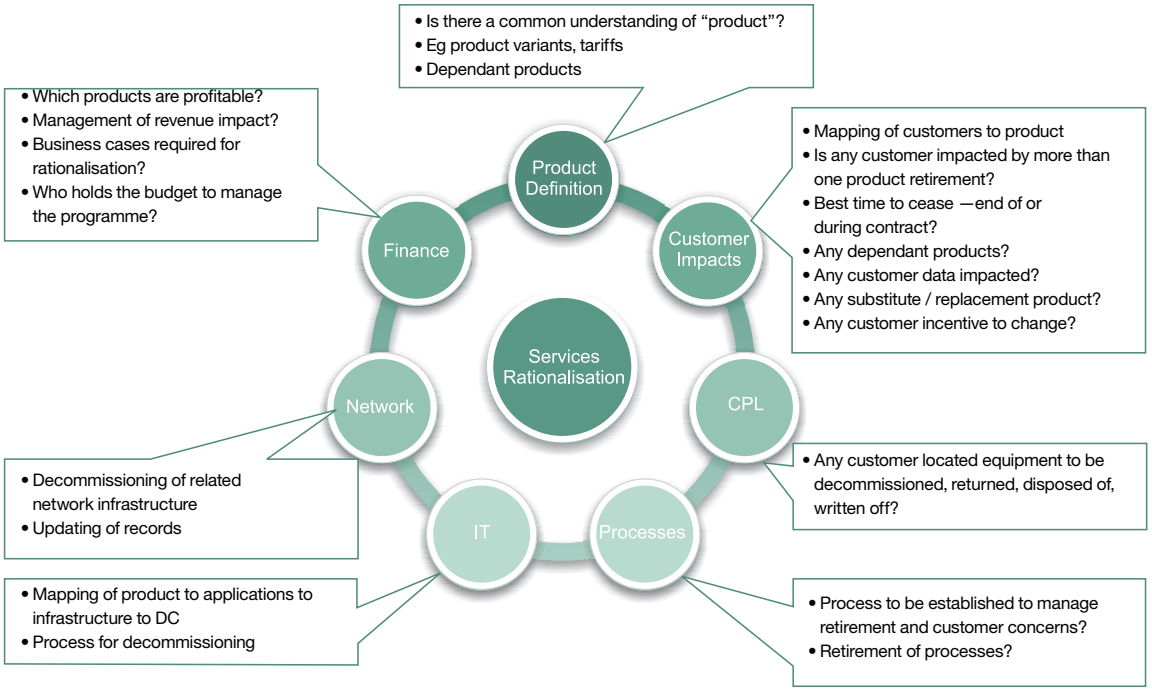


6.3.3 Strategies for carry-on or decommissioning of present services.

Strategies to apply in the decommissioning of legacy services are addressed by a practice we call 'Products and Services Rationalization'. The decommissioning of legacy services and all the coupled elements associated to each of them it is not an easy task. In the following diagram you can find an overview of different steps to be considered as part of the decommissioning of a service.

On the journey to become Digital Service Provider, there will be certain costs of decommissioning:

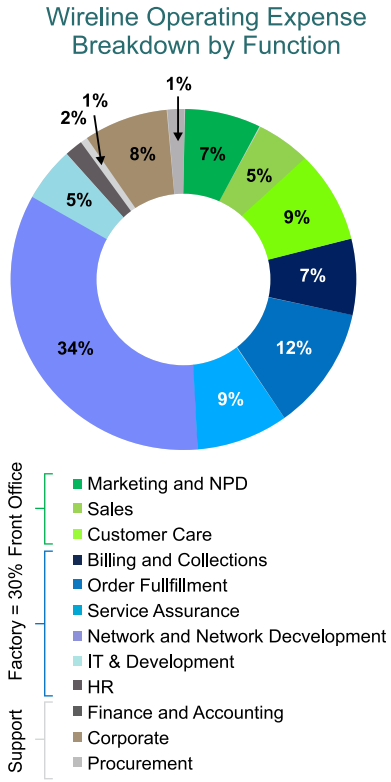
- Required investments to perform the migration of customers, including the cost associated to specific commercial migration campaigns, but also the investment required for the physical decommissioning and retirement of associated network elements and other forms of services infrastructures
- The short term degradation of revenue that is likely to arise when you engage with customers to change their services. This may result in additional churn or bundling which may increase the stickiness of the offering, but in the short term could reduce ARPU.


• Is there a common understanding of "product"?
• Eg product variants, tariffs
• Dependant products
• Which products are profitable?
• Management of revenue impact?
• Business cases required for rationalisation?
• Who holds the budget to manage the programme?
• Mapping of customers to product
• Is any customer impacted by more than one product retirement?
• Best time to cease —end of or during contract?
• Any dependant products?
• Any customer data impacted?
• Any substitute / replacement product?
• Any customer incentive to change?
Product Definition
Finance
Customer Impacts
Services Rationalisation
Network
CPL
IT
Processes
• Decommissioning of related network infrastructure
• Updating of records
• Any customer located equipment to be decommissioned, returned, disposed of, written off?
• Mapping of product to applications to infrastructure to DC
• Process for decommissioning
• Process to be established to manage retirement and customer concerns?
• Retirement of processes?

6.3.4 Changes in cost structure

The journey to become a Digital Service Provider will also require substantial changes in the cost structure of a typical CSP. Based on our benchmarking study, at the moment around 60% of the operating expenses cover what we call "Factory": network, IT, service assurance, order fulfilment and billing (see diagram on the right).

In the future, a higher proportion of the overall operating expenses will be associated with "Front office" — marketing, product development, sales and customer care. However, there will still be a need to maintain high quality of service and customer experience whilst ensuring high levels of end-to-end security.



6.4 Securing the future

Over the last decade, the pervasiveness of technology has driven change throughout nearly every facet of social interaction, commerce, business and entertainment. The impact of this shift can be found within evolving enterprise IT models, as well in the way products and services are designed and delivered to increasingly web — and mobile — centric consumers.

As technology plays a critical role in how organizations deliver value to their customers, IT security has become a challenge that represents significant organizational risk. Sophisticated attackers, cybercriminals and malicious insiders are using Internet-driven attacks to deny or disrupt service, steal sensitive business data and intellectual property, perpetrate fraud and identity theft, and gain long-term access to strategically significant networks.

Designed to gain continuous access to critical business information, targeted threats are the new reality. These attacks are well-researched, utilize cutting-edge tactics and involve custom malware that can run undetected for long periods of time. These attacks have eroded the effectiveness of traditional IT defences including firewalls and anti-virus solutions—even bypassing these controls completely in some cases.

Communication service providers play a critical role in protecting businesses and consumers from security threats including corruption, removal, disclosure, interruption and destruction of data. The critical function of network operators and the fact that they also host data on behalf of their customers means that a security breach in a CSP can create a significant ripple effect. This is reflected in security standards like ITU x.805.

For CSPs, significant changes in the mix of IT workloads are driving potential security exposure. Systems of engagement are more volatile, network workloads are being integrated and orchestrated for agility, and data has become the operator's core asset – provided it is protected from misuse and exposure.

The trend towards cloud based IT solutions that depend upon big data and are delivered to mobile devices creates a much more complex and dynamic security environment than has traditionally been the case. This gives rise to a number of current security concerns for a CSP, where the need for strict policy enforcement gives rise to requirements including:

- The ability to detect, connect and protect cloud based services that are being used in the organization, with or without the knowledge of the IT department
- An over-arching intelligence platform to provide oversight and early warnings
- Identity and access management solutions to govern and administer users and their access
- Endpoint protection for mobile users to address the "mobile blind spot" that may arise from employees using their own devices with a mixture of company and personal local apps, cloud apps, data and sign-ons.

However, there is a potential upside for CSPs. In addition to managing their own defenses, CSPs looking to deliver value-added services to enterprise clients have the opportunity to offer security services. Cloud could drive acceleration through solutions as a services in areas such as identity and access management, application security, anti-malware, security information and event management (SIEM) and data security.

In this environment, IBM believes that a fundamentally different approach to security is required—one that more completely understands and embraces the dynamic nature of attacks and the need for more integration across tools, teams and processes. The IBM approach moves beyond point products and static controls to manage a hard perimeter. It is based on dynamic technologies that approach defence through the lens of behavioural analysis.

IBM's security strategy is built on three core tenets—intelligence, integration and expertise. The result is a comprehensive security framework that spans hardware, software and services expertise, working together to provide integrated security solutions customized to meet unique needs and deliver a low cost of ownership.