> White Paper

Best Practices in Digital Transformation for Multi-Tenant Data Centers

November 2017

Sponsored by:

SIEMENS
Ingenuity for life

Management Summary

Introduction

The growth of digitalization will impact the core of the global economy in terms of the value of e-Commerce, transactions between businesses, in terms of operational efficiencies, supply chain management and the cultivation of client relationships. Companies that have used data technologies to disrupt how services and products are sold and delivered can gain competitive advantage and dominance very quickly.

Surveys conducted on the extent to which businesses are prepared for or are confident about the digital era indicate a guarded optimism about what the era will mean for business but considerable room for improved understanding and preparation. This White Paper has been prepared to define and advise on specific stages and requirements in the digital transformation process:

1. The overall process of digital transformation
2. The Internet of Things as a key function in this process,
3. The role of Analytics and
4. Underpinning any IT investment and activity, the need to ensure cybersecurity.

The focus here is on multi-tenant data centers. These are service data centers that share raised-floor space, power and cooling between tenants. They may be shared facilities leased out commercially or data centers run for client groups within a single organisation.

Digitalization is of particular relevance to MTCDs since commercial facilities beyond those offering space to the specifications required by cloud providers, managed service providers and major enterprise tenants are particularly vulnerable to the evolution of cloud which has eroded the retail client base in many markets. These MTDCs are largely unable to compete with the flexibility and scalability of cloud or with its basis of charging on the basis of what is used. The challenge to enterprise MTDCs is one step from this – the role of the on-prem data center has been eroded over the past decade partly by cloud but also by data center service providers able to offer a path to digitalization through higher specification converged facilities

Digital Transformation

No two definitions of 'digital transformation' are quite the same but most definitions share the following elements:

- It is a process involving change.
- The type of change is usually underwritten as profound or new – it is a new way of doing things not just a tinkering with the way things have been done before.
- It involves the deployment and application of digital technologies.
- The impact will be felt increasingly across business and society more generally.

Digital transformation is considered by businesses interviewed to be inevitable, enabling of opportunity, huge, far reaching, risky, unpredictable, high impact, step-by-step, never ending, transitional, progressive. It is considered also a catch-all term for a number of different components and activities – most mentioned are big data, IoT, AI, machine learning, virtual reality and augmented reality.
The reasons for pursuing digital transformation in an MTDC environment are:

- As a means of running the MTDC whether as a single facility or across a number of facilities. Given the commercial vulnerability of some of these organisations and the need to balance costs/ resources against revenues, a digital strategy is seen to improve all cost elements, improve efficiency and compliance.
- As the reason for creating a series of services that might be developed and leased/offered to clients who need the processing power and connectivity of an MTDC to formulate their own approach towards big data, IoT or other elements of digital transformation.

The cornerstones of digital transformation are seen to enhance the nature and purpose of the MTDC:

- Data becomes central to the organisation.
- Through the process, all companies become de facto technology companies.
- That while the emphasis is on the deployment of technologies, the strategies for this are based clearly on the business requirements such deployments are intended to meet.

Digital transformation is considered as a long term proposition therefore best practice can be used as a means to progress through the steps through which a strategy to coordinate the requirements of the company with the capabilities of technology can be developed and implemented. The strategy will progress through stages of project-by-project application towards one where all of the company is drawn together, and it will become increasingly more proactive in enabling the company to become a disruptive force in its own right.

As businesses move towards multiple environments to meet their IT needs and move away from the data center towards the concept of data infrastructure (in which MTDCs usually play a role) so there needs to be visibility and coordination across different parts of the infrastructure and the networking, computing and storage functions.▶

▶ So, what does digital transformation mean for MTDCs? The impacts will be far reaching in terms of changed requirements and expectations customers have for more demand-driven, scalable and efficient infrastructure that operates on the basis of intelligent management and real time modeling, where the company and the partners it may need to bring in are synchronized around data and analytics.

The Internet of Things & the MTDC

Dealing with IoT and capitalising on the opportunities it presents is a core element of digital transformation for MTDCs if they can effectively harness it, since it offers insight that can transform the way employees, suppliers, customers, products and processes are understood and how facilities are designed and operated.
IoT is a key part of digital transformation. For the MTDC it will extend the knowledge of and interaction with clients and lead to more effective decision making in relation to them. It will also facilitate that process in relation to external links into the data center such as networks and other components of a client's data infrastructure if the MTDC is to act as the core control point of that infrastructure. The situations in which IoT can be of greatest value to the data center will reflect the previously stated transformation strategy and include operations, CRM, business development, infrastructure utilization, virtualization, capacity planning, operating systems and data products. Depending on the business opportunity to be realised, an MTDC may need to implement a number of IoT technologies and strategies.

The deployment of IoT will require sensors at the point where data is collected, sensor technology to manage and direct the sensors, RFID tags, embedded systems technology, IoT analytics and the means of acting on the findings.

The need to capture, process, store and analyse data to generate corporate value has generated the emergence of a new breed of technologies. Critical to the process of using IoT are two main categories of technology – for storage given the huge amount of data involved, and processing.

Efficient use of IoT in this context requires the data source to be defined. All elements of the MTDC including infrastructure, IT, storage, networks and security may be relevant data sources to examine. Each of them provides valuable information for understanding the performance of infrastructure and enables infrastructure to be optimised. Ultimately, machine and software data is the key to unlocking analytic applications.

In addition to the operational deployment of IoT, since the data center is the source of business rather than just the enabler and the clients are inside the facility rather than outside, so the IoT needs to be related back to individual customer, budgetary and contractual objectives.

Analytics

Analytics is the extensive use of data, statistical and quantitative analysis, explanatory and predictive models, and fact-based management to drive decisions and actions. Analytics can be the input used for human decision-making or it may drive fully automated decisions. In short, analytics enables decision-making based on data and evidence, rather than speculation and 'hunch'. Analytics is important because data on its own is simply a set of numbers, words, images, sounds or other symbols. Data itself needs to be transformed to be able to be useful.

There are many benefits of deploying analytics for IoT within the data center. These are linked with the reasons for deploying IoT since analytics forms the processing component of the data generated by IoT. The benefits can be described in terms of the evolution of strategy through different types of analysis including description, diagnosis, prediction, prescription and prevention. MTDCs need a structured, actionable path toward optimising their facilities in terms of business objectives by leveraging data and analytics for their decision-making. That means defining specific objectives based on corporate requirements, determining the scope of the analytics strategy, creating a team of experts, defining an improvement process methodology, and selecting and implementing the right tools, technologies and data integration methodologies.

The scarcity of data related to the data center will no longer be the characteristic that defines MTDC efforts to understand their data centers. There are significant issues that accompany the deployment of analytics and which determine its use in future decision making, whether human or AI-based including data generation, data quality and reliability, data curation, data capture, processing and storage.

The whole process leading to analytics requires the company to identify the clear business goals that drive their data center management. Analytics will necessarily be a long term strategy. The application of analytics provides the opportunity of continuous improvement in the MTDC data center in all aspects. In a traditionally facility-oriented organisation, the IT department is going to need more employees, not fewer. Big data analytics requires a new breed of experts in the DevOps team, namely a data scientist. ▶

Security

The operators of MTDCs are faced with the tasks of securing growing and evolving network architectures against increasingly sophisticated and targeted attacks, while at the same time meeting ever more stringent compliance and regulatory requirements to protect the data with which they are entrusted.

This includes threats on the cyber level such as DDoS attacks, web application attacks such as SQL injection and cross-site scripting, ransomware (where data is held for ransom supposedly until a ransom is paid). DNS infrastructure attacks, malware including Trojans, viruses and worms, phishing, unpatched software, social media threats and advanced persistent threats (APTs) via (spear) phishing. Just like natural viruses which mutate in order to survive against antibiotics, so the list above will mutate and combine in order to present a more sustained and complex mode of attack.

While the focus of security has moved to cyber-threats based on the changing profile of the data infrastructure landscape, other sources of disruption should not be ignored. Hacking, malware and threats delivered via social media have grown the most to 2015 in terms of numbers while physical, environmental and disruptions caused by error and 'misuse' have remained at a consistent level. This cluster of threats remain at a level however where they cannot be ignored. There are a number of important considerations for developing a security model in an MTDC:

- It needs to reflect the changing design and operation of a multi-tenant facility and be designed for the mix of services and environment offered by the facility (or facilities).
- It must be able to adapt so that it provides consistent, constant and intelligent protection across evolving and hybrid data center models.
- It must provide protection against advanced and evolving threats.
- It will only be as strong as its weakest link therefore it needs to observe principles of 'absolute' protection, described as 'End to end', 'Layered' or 'Zero Trust' depending on the form of security.

It is evident that traditional network-centric security systems based on perimeters and firewalls are no longer adequate for any but the most legacy MTDC. Traditional security policies are defined for security zones that are static and tied to physical devices, and which are signature-based. Although these have evolved to next-generation firewalls (NGFWs) that can implement policies based on applications, users and content, they are still static and rely on traditional network constructs like IP addresses, virtual local area networks (VLANs) and server zones. Traditional defenses like firewalls, IPS, anti-virus and gateways are simply no match for continually evolving and sophisticated cyber threats, which can blend malicious techniques.

The MTDC environment is now software-defined, distributed, interconnected, dynamic and user-focused. The cybersecurity risk to the service data center is made worse by dependence on virtualization, cloud computing and the internet of things (IoT). This creates a complex and dynamic network that gives more opportunities for attackers to compromise a facility.

It now widely accepted that security must be deployed throughout an organisation's data infrastructure, and out to the growing number of endpoints that are connected to that infrastructure and used to access cloud services. There also needs to be greater visibility into the network, as well as enhanced segmentation and control. There are two key methodologies in securing the next-generation network and everything connected to it. The first involves reducing the attack surface and, the second involves mitigating the risk. However, there are numerous different - but often parallel - approaches to both.

Reducing the attack surface aims to prevent all but authorised access to system assets, and to establish access rights. This can be achieved by minimising exposed system targets, controlling system and network segment access across the network, enforcing least privilege for all security subjects, or reducing the amount of data that needs to be scanned by deploying trusted software and procedures.

In order to mitigate the risk of attacks, the MTDC provider must also understand the risks and then implement specific measures to reduce or minimise unacceptable risk, such as those to reduce the severity of the consequences of an attack, reduce the probability of an attack occurring, or reducing exposure to the attack. This might include traffic segmentation to filter and verify network activity to reduce the potential attack surface include firewalls and switch access control lists (ACLs), as well as the creation of subnets and logical segmentation for internal traffic and gain visibility into applications, users and content.

Security must work across the multi-tenant data center so that client organisations can rest assured that their data and applications are safe. This means a consistent and accurate security policy across heterogeneous environments. The programmability aspect of new security technologies is all software-based. Indeed the majority rely solely or to a large extent on software.

Software-Defined Security is adaptive in that the security policy and controls automatically remain with the device if is moved, migrated or scaled, which speeds up response time and reduces the scope for human error.

Increasingly, sophisticated algorithm-based techniques are used, not just to identify security threats but to diagnose the wider principle of 'data health'. There are two main aspects to threat intelligence: technology or machine intelligence, and human intelligence. While machine intelligence is able to mine and analyse ▶

▶enormous amounts of data in real-time, many in the industry believe that it is not enough, and that human input is needed to refine the findings.

Threat intelligence seeks to detect anomalies, by establishing a baseline of normal behavior so that abnormalities can be detected through the use of user behavior and user analytics.

Threat intelligence also looks to identify "indicators of compromise". These are the tools, techniques and procedures used by attackers from the artifacts left behind in an attack. From this intelligence, countermeasures can be implemented to prohibit future attacks. Techniques here include Network Anomaly Detection which is the action of finding behaviors in network traffic which do not conform to expected patterns and Root Cause Isolation Root Cause Isolation (RCI) which is the process of identifying the source of anomalies (potentially problems) in a system using only data observation.

Root-Cause analysis involves an automatic investigation of problem KPIs and diagnosis regarding failure reasons through the automation of the diagnosis process by creating models per cell, KPI and area to identify the component leading the anomaly.

Much recent media attention on data center security has focused on the threat of disruption caused by malware, targeted DDoS and other electronic forms of assault. Yet focussing efforts purely on combatting unseen, stealth attacks from digital sources can draw attention away from the threat of physical attacks on, or accidental damage to, premises and equipment.

Multi-tenant facilities and colocation give business agreed levels of freedom to manage their own software and hardware in a controlled environment, possibly sharing access to server rooms to carry out upgrades, repairs, new installations, and routine maintenance. That increases the volume of traffic, vehicle and human, travelling in and out of the facility. This has the possibility of increasing the threat of disruption if not carefully and securely managed.

There are two related principles that apply to the physical protection of the data center. The first is 'defense in depth', that is to ensure protection is backed up so that if it fails at one point then there is a further defense behind that, and 'layered' security. As data centers need to provide access as well as defense, a key component of security is the need to organise it around a series of points at which further access is allowed or denied to someone seeking entry to the facility.

There will be the continuing need to deploy available security measures to protect the data center that may include perimeter walls, embankments and fences, multiple security checkpoints, manned security stations, mantraps, biometric readers., keeping the building away from the perimeter, keeping equipment racks away from any external walls and away from windows, surveillance networks covering both internal and external areas and perimeters, intruder/fire alarm and control systems, lockable racks and cages in multi-tenanted environments, fire-proofed/air-locked doors, powder fire extinguishers, a gas based building wide fire suppression systems and access controls. Further advances based on facial or retinal recognition, the deployment of AI to drive access and security systems, technological improvements around CCTV, motion detection, the remote control of locking mechanisms, the use of laser technologies to create beams that provide a barrier to a protected zone can be deployed as they are developed. ●

DCD Comment

The ongoing digital transformation of economies globally should represent a major opportunity for multi-tenant data centers across both the enterprise and shared data center sectors. The data center is the cornerstone of digital transformation processes since at least in a post-legacy configuration it offers the processing, storage and network capacity to enable those processes to occur. Colocation providers have historically offered enterprise a higher spec'd and more cost-effective data center option than building or refreshing an in-house data center and as few enterprise data centers will be able to deal on their own with the requirements of digital transformation. Yet digital transformation does not mean the disappearance of the enterprise data center but it means a changed role based on its processing, storage and networking specifications.

MTDCs see digital transformation as an opportunity and a considerable challenge. Whether enterprise or service facility, the majority of MTDCs cluster at the slower end of an adoption spectrum, conducting piecemeal projects and are still to embark on the holistic re-setting of their company that transformation looks for. The data center as centerpiece of the digital business may act as a brake – since the compute requirements for the company's own IoT and analytics is compute that is not available for client use.

Most MTDCs (in particular smaller local and regional operators) have evolved relatively recently out of their own legacy era of being based on space, racks, power and connectivity whether on-prem or outsourced. While there is now a considerable move towards services and, in situations where the facility offers sufficient levels of scalability, convergence and control, there is also a trend towards offering cloud. Across the MTDC sector there are a variety of business models, contractual arrangements and delivery methods and no consistent path whereby MTDCs achieve their own digital transformation.

However MTDCs have devised a number of different ways to deal with the major threat to their customer base – cloud. These ways include developing their own (if they have the capacity and expertise), buying into private cloud and developing hybrid cloud models, accessing it through interconnectivity or through their facility eco-system, or through other forms of partnership since cloud providers outside the global giants rely on service facilities to house their cloud bases. The approach to IoT, analytic and security will be similar, particularly in the need to develop strong partnerships and expertise in updating not only their technological capacity but their business models. As with any digital transformation the process returns technology back to the business. ●

Contents

Introduction

This White Paper has been written on behalf of Siemens in order to identify and analyse key trends in digital transformation as these relate to multi-tenant data centers [MTDCs].

The information presented in this report has been collected from a number of sources including interviews conducted specifically in relation to this project, together with analysis of data collected as part of the DCD Annual Data Center Census as well as surveys, media reports and analyses provided by independent experts. The DCD Global Census has collected annually over 2,000 responses from end-user organisations and 500 from colocation, cloud and hosting providers.

In this Paper, digitalization has been used as a term to represent the digital transformation of a business to change business models and to increase competitive opportunity, in contrast to digitization which is the process of converting analogue information into a numerical format.

Comments shown in italics come from the 12 depth interviews that were conducted as part of the research input to this Paper. The type of organisation is also indicated. ●

Analysis & Discussion

Why 'Best Practice'

The statistics that herald the continuing rise of the digital age are well-known. To pick a selection of the most quoted: 4 billion searches a day (Google), 500 million tweets (Twitter), 254 million orders in a day (Alibaba), 350 million new photos per day (Facebook), 235 million messages per day (Tencent QQ). According to Cisco's Global Cloud Index (2015), global data center IP traffic will grow at a CAGR of 27% between 2015 and 2020 to 15.3 Zettabytes per annum according to Cisco, and there will be as many as 25 billion devices connected to the Internet of Things (IoT).

The growth of digitalization extends wider than social media and it will impact the core of the global economy:

- eCommerce will double as proportion of retail sales worldwide from 7.4% in 2015 to 14.6% in 2020 at a value of over USD $4 trillion. This figure, quoted in eMarketer at August 2016 does not include travel and event tickets. While it may not seem as spectacular as some statistics associated with the digital era, retail is the largest area of commercial activity in the world – the data includes areas of the world with limited Internet coverage and even more limited eCommerce capabilities and goods less suited for eCommerce, for example, perishables and foods which are the largest area of retail.
- Global B2B E-commerce will reach USD 6.7 trillion by 2020, according to Frost & Sullivan. The rate of increase (based on US analysis published by Forbes) of B2B will increase at double the rate of B2C.

The disruption can be demonstrated by comparison between some of the organisations which have been seen as disruptors, those which they have displaced, and the progress of the existing market since disruption. Do note that many other factors may also influence what has happened to the previous market and its key players so the information should not be read as correlating directly. It should also be noted that disruption in some cases grows or creates markets, rather than just displacing incumbents: ▶

Figure 1: The Impact of Technological Disruption

Market	Disruptor	Key Statistic	Measure	Incumbent	Impact
Taxi services	Uber	2.93 (2014) > 20 (2016)	Gross global revenue USD billion (leaked)	Fall in income of 10% among established drivers (Benedikt Frey, OMS, 2017)	Uber appears to have grown rather than reduced driving jobs in cities where it operates, the better income stats for Uber drivers are because platform allows more effective use of driver time
Retail	Amazon	1.2% (March 2013) > 5% (March 2017)	Share of US retail market for categories served by Amazon	Sales from store-based retailers grew by only 0.8% in Q1 2017 indicating trending decline	Considered the classic disruption case study – Borders (book seller) filed for bankruptcy in 2011
Accommodation	AirBNB	July 2012: 4 > end 2016: 55	Google search index data	Hilton: 100 > 85; Marriott: 80 > 65; Expedia: 63> 55	From just over 1% of US supply at end 2014 to 5.5% in March 2017
Home Entertainment	Netflix	100 million subscribers	As at July 2017	Various in DVD and entertainment supply chain, sales of DVD players have declined from 2006. Revenue from video streaming is now 9 times that from DVD rental/purchase.	Bankrupcy of Blockbuter. Netflix listed for 91 Emmys in 2017.

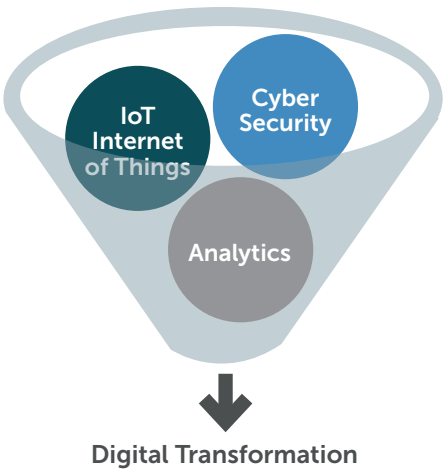
Source: Corporate & Media Reports; DCD 2017

▶ Surveys conducted on the extent to which businesses are prepared for or are confident about the digital era indicate a guarded optimism about what the era will mean for business but considerable room for improved understanding and preparation across different areas of the world:

- A survey conducted by Siemens among 300 executives of client companies in the UAE and Qatar indicate that 45% consider themselves familiar with what digital transformation is but 77% associate it with the adoption of a single technology. Only 37% have a digital strategy and 1% have a Chief Digital Officer or an equivalent person leading digital initiatives.
- Half of the CEOs responding to Gartner's 2016 CIO survey expect their industry to be substantially or unrecognisably changed by digital but that "some CIOs find themselves ill-prepared to lead in the ways demanded by the impending digital reality".
- The Fujitsu Global Digital Transformation Report of February 2017 indicates that 89% of business leaders respond that their company is planning, testing and implementing digital transformation projects and that 34% of these projects have generated positive outcomes.
- The Forbes Alfresco survey reported in August 2017 based on 328 senior-level executives in North America and Western Europe indicates that 83% of fast growing companies (=a growth of 10% or more based on earnings before interest, taxes, depreciation and amortization). have a dedicated UX team for digital transformation compared to 47% of those with lower growth.
- 80% of business leaders in the Asia Pacific believe they need to transform to a digital business to enable future growth [Microsoft Asia Digital Transformation Study, February 2017] yet only 29% said that they had a full digital strategy in place.

Among DCD samples of companies with sufficient IT workloads to require access to a data center, the adoption of digital technologies to replace legacy ones is, at 2016, still a work in progress with the exception of server virtualization which is the longest established option shown on the chart below. By 2020 digital options will have advanced further particularly the deployment of public cloud and services access from it, but the level of upgrades will also rise, indicating that the on-premise environment will continue, usually as part of a hybrid IT arrangement.

Figure 3: The Key Components of Digital Transformation

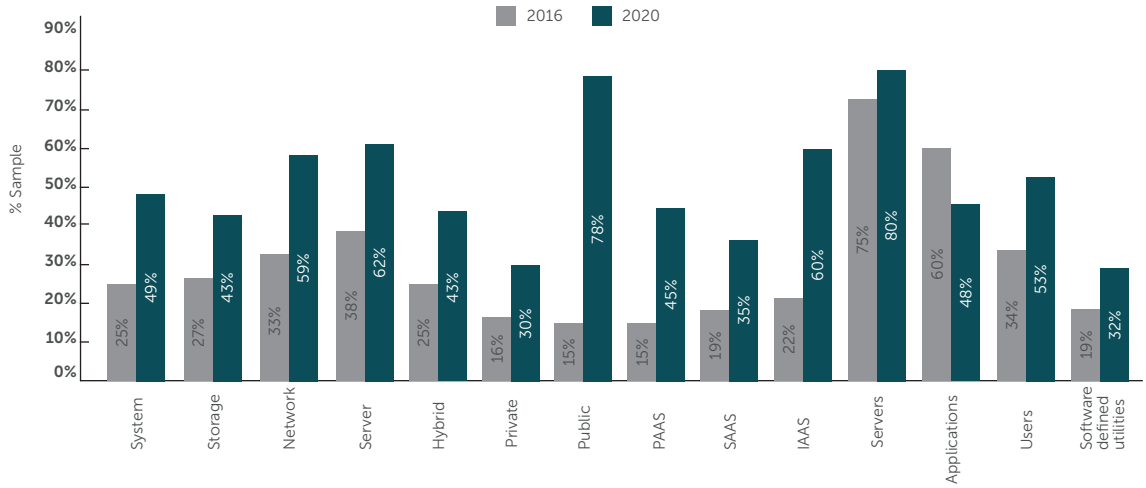


Source: DCD 2017

This White Paper has been prepared to define and advise on specific stages and requirements in the digital transformation process:

1. The overall process of digital transformation
2. The Internet of Things as a key function in this process,
3. The role of Analytics, and
4. Underpinning any IT investment and activity, the need to ensure cybersecurity. ●

Figure 2: The Preparation for Transformation within Data Centers



Source: DCD Solutions Survey 2016

Why Multi-Tenant Data Centers?

This White Paper has been prepared with a focus on multi-tenant data centers. These are service data centers run either for clients external to the provider ('commercial') or clients within a company ('enterprise'). These facilities share raised-floor space, power and cooling between tenants. The portfolio of such facilities may include a variety of standalone data centers, server rooms and disaster recovery sites. They may be built as a campus, as a dedicated purpose-built facility or, in a building shared with other commercial or industrial activities. Provision is made for underground utility feeds, diverse fiber entrances, the capacity for diesel storage and for physical security.

In commercial facilities, space may be offered from units as small as the sub-division of a rack, through whole cabinets in open floor areas, through secured and separated cages which tend to be located on the main floor area and suites which may be separate from the main floor area.

According to DCD research there are around 1,650 organisations worldwide who offer MTDC facilities on a commercial basis. They operate around 7,500 facilities which have collectively around 8 million square metres of white space. In 2016 they invested around US$22 billion in their facilities (around 30% of all investment in facilities). This will rise to US$40 billion in 2020 (36%). The 50 largest MTDC operators account for around 35% of the asset base and of investment activity. The number of enterprise MTDCs is far larger although these facilities are less likely to be purpose built and they will tend to be smaller.

There are a number of reasons why the issues of digitalization is of particular relevance to MTCDs.

Both colocation and enterprise MTDCs are vulnerable to the loss of their customer base to cloud. Colocation providers which have focused more on a wholesale offering have largely been able to navigate through the challenge of cloud by offering single tenant space to the specifications required by cloud providers, managed service providers and major enterprise tenants. The MTDC world is populated by smaller companies and considerable takeover activity and market rationalisation. Cloud has eroded the SME client base in all but the most recently established 'emerging' markets (due there to the unavailability of suitable cloud or IT services). MTDCs are largely unable to compete with the flexibility and scalability of cloud or with its practice of charging on the basis of what is used.

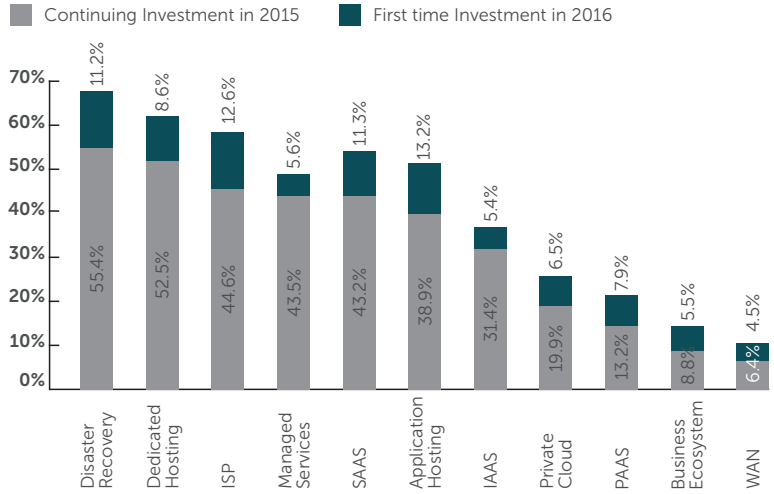
"I'm not sure what the future holds, to be honest. Cloud is everywhere and offering everything. It has cut down the deals that we do – deals we used to do for 40 racks are now for 10"
[IT services]

The enterprise MTDC is vulnerable both to cloud and to other forms of outsourcing. This has led to the continual erosion of the in-house/enterprise asset base over the past 6 or 7 years. While corporate preference, legislation and security requirements keep a large number of enterprise MTDCs alive, the companies that rely on them know that they need to develop technologically in order to remain relevant.

The response among all types and sizes of MTDC is to move from a facility that is operated or leased on the basis of racks, power, connectivity and security to one that offers access to services either through in-house ecosystems or through various modes of cross-connectivity. Not all MTDCs particularly in the enterprise sector have the facility profile to do this effectively, but colocation providers are able to offer a business case based on the argument that it is more cost effective to access a range of IT and cloud services via a facility that is able to do so than to upgrade an on-prem. data center at considerable cost.

A majority of MTDCs offer disaster recovery services, access to ISPs, dedicated hosting, application hosting and SaaS. This indicates a fundamental transition from a business model based on infrastructure rental, to one based on IT resource rental based on interconnectivity and then to a model offering IT resource as application services based on cloud infrastructure. Different MTDCs are at different points along this spectrum. Some have had no need to move away from the original colocation model (space, power, connectivity, security) while others will have moved through the spectrum. ▶

Figure 4: Investment in IT & Cloud Services & Solutions 2015 & 2016: % Sample of MTDCs



Source: DCD Census 2014 & DCD Solutions Survey 2016

▶The transition from colocation towards IT and cloud based service models and is rarely straightforward or the same journey between different companies. It is made more complicated by three factors:

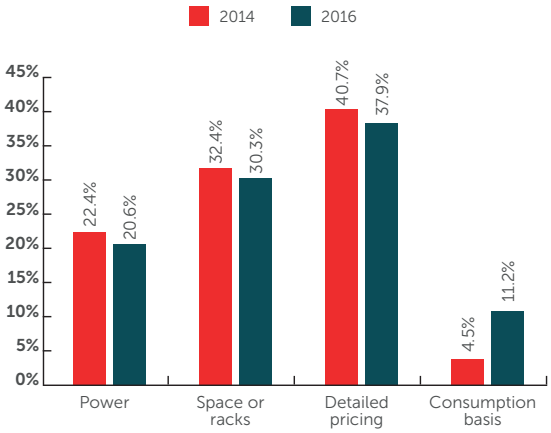
1. The means of offering IT resources and services will vary. For larger MTDC companies a branded delivery model will be developed in-house. For MTDCs without this level of expertise or resource, services can be developed through partnerships, through mutually beneficial commercial arrangements (offering space in return for the capability to market and offer services), through an 'ecosystem' or through other referral arrangements. These arrangements are assisted by the fact that, outside the larger cloud, internet and managed service providers, these sectors rely on commercial MTDCs for data center space.

"Some of the systems that we manage are client owned, we treat these are part of our own hosted systems in terms of the way we govern their operation. Then we have cloud services – some of which are contractually owned by clients and some by us and simply resold. Across each service model we have varied delivery methods – we tend to have a dedicated IT team for each contract and for each major location. We have a strengthening affinity with cloud delivery and seek to deliver cost savings for clients by ensuring we maximise the use of cloud systems that have proven to reduce costs and maintain high service availability." [IT services]

"We are looking to develop a more converged, networked and efficient environment that will be able to meet the demands of private and hybrid cloud, run software-defined with a clear management and operational system. The enterprise data center fights back." [Financial sector]

2. The method by which MTDCs charge for their facilities and services is in a state of flux. In enterprise MTDCs servicing internal clients, there may not be charging and this has always been given as a reason for slow progress on energy efficiency. While there is a move to charging on the basis of consumption to compete on a more level playing field with cloud, around half of commercial MTDCs in the 2016 sample are still using power, space or racks as the basis of charging. Usually services or interconnect are added if/as used to the basic facility charging model.

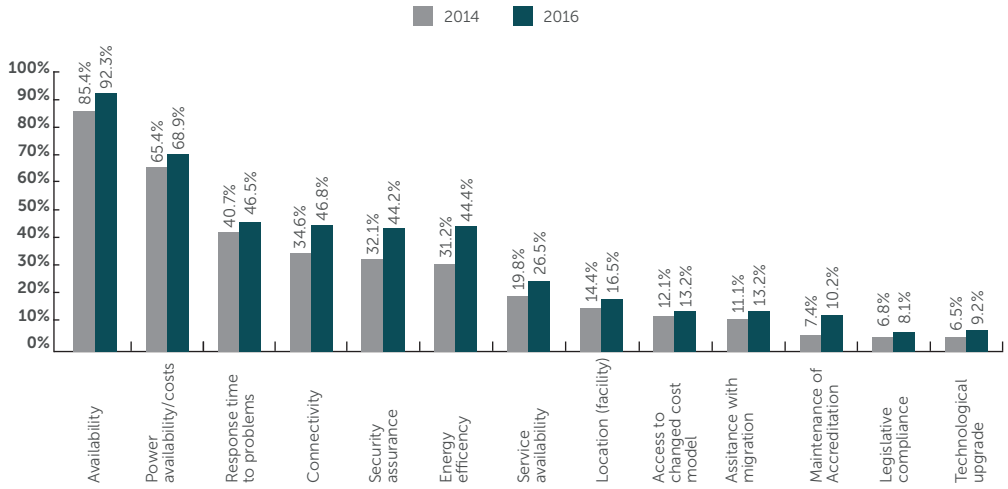
Figure 5: Main Method of Charging 2014 & 2016: % Sample of Commercial MTDCs



Source: DCD Census 2014 & DCD Solutions Survey 2016

3. A number of criteria are built into the service level agreements which determine what the commercial MTDC will provide to the client. SLAs tend to be building in more criteria (and usually over shorter periods of time). While most will deal with an agreed level of availability for service and with power provision, there are a range of other issues. This again will add to the complexity of managing a MTDC and keeping it profitable. ▶

Figure 6: Components in MTDC Service Level Agreements & Contracts 2014 & 2016: % Sample of Commercial MTDCs



Source: DCD Census 2014 & DCD Solutions Survey 2016

▶ To remain relevant to its client base, the MTDC sector needs to recognise the trends in data infrastructure as digital transformation impacts enterprise. These may include:

- The deployment of hybrid or multi-cloud environments to achieve necessary levels of scalability, security, reliability and the flexibility to meet changing business strategies. Under this system, more sensitive data applications can be kept in a private cloud environment built via IaaS infrastructure and Open Stack programs with a monitoring and operations program and a supporting service system.
- Integration of public cloud via transition from IaaS to PaaS service, resource pool expansion and optimisation of platform availability and management.
- Rapid innovation may be assisted using SaaS services for enterprise applications.
- IoT will form the basis of the connection and the sharing of knowledge between the business, its clients, its staff, its suppliers. IoT product programs are maturing and the IoT platform can build interoperability with enterprise cloud platforms and the DMP platform and be used to develop business applications.
- The data management platform and an integrated data center management suite is the core of digital transformation.

The MTDC wishing to capitalise on the direction in which many customers will move need to be aware of the transformational paradigm above and others like it since the processes it entails may represent opportunity (or challenge) for the MTDC.

"Colocation is the preferred choice for a lot of enterprise architecture and cloud is their preference for desktop and SaaS type applications such as email, mobility, collaboration & communications etc. Then there is a layer of internal systems that they can't easily migrate – call those legacy IT – they may be in our facilities or they may be on premise." [IT Services]

"We operate a number of data centers that host private cloud services that customers use to deliver a number of services. The applications that demand the greatest scalability, such as CRM and general enterprise applications are hosted within these data centers. We also have a relationship with a number of providers of cloud services – in particular SaaS vendors." [IT Services] ●

'Digital Transformation'

No two definitions of 'digital transformation' are quite the same but most definitions share the following elements:

- It is a process involving change.
- The type of change is usually underwritten as profound or new – it is a new way of doing things not just a tinkering with the way things have been done before.
- It involves the deployment and application of digital technologies.
- The impact will be felt increasingly across business and society more generally.

While the term is understood, it is considered open-ended. This perception is caused by the huge perceived scope of digital transformation:

"If it's done properly, it's everything. It's almost like you are handing over control of the company". [Business Services]

"If you look at Uber, Amazon, Facebook, they seemed to come from nowhere and build vast empires. They are basically IT companies that have extended into areas of necessity and taken it over." [Personal Services]

Digital transformation is considered to be (among other adjectives used) inevitable, enabling of opportunity, huge, far reaching, risky, unpredictable, high impact, step-by-step, never ending, transitional, progressive. These adjectives indicate positive, neutral and some negative sentiment and a high level of caution.

It is considered also a catch-all term for a number of different components and activities – most mentioned are big data, IoT, AI, machine learning, virtual reality and augmented reality. It is seen as a combination of some or all of these activities in combination, and finding the right balance between them is seen as a major challenge. Since digital transformation is such as considerable activity, questions are raised as to how far it can be measured so progress can be ascertained.

The reasons for pursuing digital transformation in an MTDC environment embrace two main drivers:

- As a means of running the MTDC whether as a single facility or across a number of facilities. Given the commercial vulnerability of some of these organisations and the need to balance costs/resources against revenues, a digital strategy is seen to improve all cost elements, improve efficiency and compliance. Mention is made in this context of Google's use of algorithms to improve operational efficiency. Thus, digital transformation is seen to have internal value.
- As the reason for generating a series of services that might be developed and leased/offered to clients who need the processing power and connectivity of an MTDC to formulate their own approach towards big data, IoT or other elements of digital transformation. These include the components outlined above in the way an enterprise organisation might approach digital transformation.

"They come to us for what I'd call heavy data processing where they need to connect with cloud infrastructure to augment their internal processing capacity. They can get this capacity in a highly elastic environment much more economically from us." [IT Services]

"Everything is really up in the air as I look at what we do here and think that it may all get disrupted. It pushes us to change the way we do our business, interact with our customers, learn about them, everything. Or is it just a tech sales gimmick? But I doubt that". [Business Services]

"One of our key market differentiators is technology. We sell our services as an alternative to in-house fulfilment of logistics services and their offering is based largely around the efficiencies that smart technology can bring to the process." [Business Services]

Analysts and MTDCs agree that the path to digital transformation enhances the nature and purpose of the MTDC provider:

- Data becomes central to the organisation. A recent DCD study around Industry 4.0 indicates that data is now more valuable to manufacturing and process industries than any other resource.
- Through the process, all companies become de facto technology companies.
- That while the emphasis is on the deployment of technologies, the strategies for this are based clearly on the business requirements such deployments are intended to meet. This is not technology for technology's sake.

Figures quoted for the progression of digital transformation are emphatic. According to Gartner, 80% of the business sectors of enterprise will participate in IT construction. The proportion of the CIO budget spent on digitalization will rise to 28% by 2018. By next year, two-thirds of the CEOs of Global 2000 enterprises will have digital transformation at the core of their corporate strategy. A KMPG study of 2016 ("The disruptors are the disrupted") indicates that 67% of tech leaders surveyed believe that disruptive technologies are having a positive impact on their company's performance. Again there is a proviso – less than one-third of these technology companies are very prepared for disruptive technology.

By 2021, the global digital transformation market will be worth an estimated USD 392 billion and by 2020 they have the potential to add as much as USD 1.36 trillion to the GDP of the world's top 10 economies. According to IDC, the worldwide market for IoT solutions will grow to USD 7.1 trillion by 2020. ▶

▶Digital transformation is considered as a long term proposition therefore best practice can be used as a means to progress through the steps through which a strategy to coordinate the requirements of the company with the capabilities of technology can be developed and implemented. The strategy will progress through stages of project-by-project application towards one where all of the company is drawn together, and it will become increasingly more proactive in enabling the company to become a disruptive force in its own right:

Figure 7: The Digital Transformation Critical Path

Source: DCD 2017

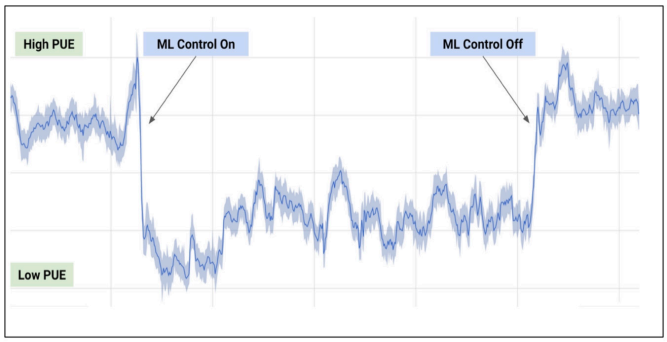
Within each stage of progression the implementation of 'best practice' can be represented by a process of:

1. Planning: in order to establish targets, responsibilities and process
2. Mapping: ensuring that decisions reflect the objectives established through planning, through mapping the IT outcomes onto the corporate requirements
3. Decision making: making the correct choice of technology for the process
4. Implementation of the transformation
5. Review/learning to feed back into future strategies.

So, in what situations have data centers (of whatever kind) developed and applied digital transformation strategies?

Google has since 2011 developed algorithms to improve the accuracy and relevance of their search functions. Within its data centers, it has used DeepMind AI to cut its data center energy bills by putting the AI system in charge of power use in parts of its data centers. This has led to a reduced requirement of power for cooling which is in most Data centers, the largest non-IT consumer of power. To achieve this, the neural networks control around 120 variables and takes data from sensors located across the server racks. The system is self-improving – the analysis of data allows further sensors to be deployed to improve the accuracy of the intelligence. Google claimed to have achieved a PUE of 1.12 across its Data centers by 2014, an average that it has maintained into 2017.

Figure 8: The Deployment of AI to Improve Energy Efficiency in Google Data Centers



Source: Google

As businesses move towards multiple environments to meet their IT needs and move away from the data center towards the concept of data infrastructure (in which MTDCs usually play a role) so there needs to be visibility and coordination across different parts of the infrastructure and the networking, computing and storage functions.

For the MTDC, profitability is based on minimising wastage in particular of resources that form part of the business model – space, power, networks.

"It's about controlling costs, looking especially at cooling and power but as the operation becomes more complex so there are a lot of possible sources of cost. Money that cannot be charged back comes off the bottom line." [IT Services]

"*We are getting real pressure from the top – we need to cut costs in the data center and improve efficiency. It's strange – as our data center becomes more valuable so it becomes more of a focus of cost cutting*". [Financial Services]

This is the monitoring role that has been fulfilled in the past by a variety of technologies including DCIM software, building management systems [BMS] and systems provided by infrastructure suppliers for their suite of products. DCIM has evolved in line with changing data center profiles to take data from both the infrastructure and IT stacks and analyse it to facilitate efficiency and quality of operations.

As the data center becomes more digitized in terms of its infrastructure stack – through equipment that is coordinated and managed through operational systems, through the software defined systems adopted to reduce the costs of infrastructure, improve efficiency and to act as the most effective access into cloud systems. Software-defined infrastructure (SDI) can be defined as technical computing infrastructure entirely under the control of software with no operator or human intervention. It operates independent of any hardware-specific dependencies. ▶

▶ So, what does digital transformation mean for MTDCs? As with any other commercial organisations, the impacts will be far reaching:

1. Most critically the requirements and expectations of customers will change. The foundations for digital transformation will be the business strategy and usually these are based on meeting customer requirements profitably. Just as the customers of the MTDC will be facing disruption so will the MTDC itself.
2. The commercial MTDC needs as colocation has always done to run parallel to the evolution of enterprise data infrastructure. This means the development of off-prem private cloud, interconnection to public cloud providers, the hosting as necessary of the client company's migration into SaaS and platform development. It is quite possible that some of this transformation will require more scalable and efficient infrastructure than is available in-house and therefore this will bring in MTDCs. The attitudes expressed to digital transformation as a series of future uncertainties means that a managed cloud service component may be of value.

"We divide our IT into 2 parts – the first are internal systems which we keep in house, the second tend to use cloud based solutions because of the flexibility." [Developer]

"Colocation is the preferred choice for a lot of enterprise architecture. Cloud is the preference for desktop and SaaS type applications – email, mobility, collaboration & communications etc. Then there is a layer of internal systems that can't easily be migrated – call those legacy IT that we are formulating a strategy to deal with – they may be in colocation facilities or they may be on premise. High performance computing is currently all on premise and is likely to stay that way – we can deliver that at a lower cost currently than we would achieve externally – if it was possible to buy from a cloud vendor at all. We have a real estate division and we effectively lease the space from them – but to every intent it is an internal operation." [Primary Industry]

"I think we will need to look more closely at a number of outsourcing options and experts so we can manage all of this." [Business Services]

3. Digital transformation will also mean that the facilities offered by MTDCs will need to evolve into service hubs where the key operational principles are demand-driven, offering flexibility and scalability. The major applications of transformative technologies in data centers to date have been in operations and management but the technology now has the potential to take this further. The MTDC as a 'one size fits all' proposition will not survive much longer, therefore one key disruption will be to evolve a standard of intelligent management that allows the facility to customise the requirement to meet customer needs. This process has started already in terms of variable Tier levels, different levels of separation and security, different service profiles and more open systems but emerging technologies can be used to get this to a stage where it is genuinely on-demand and where, through the application of AI and machine learning it may be based on a level of demand that the client themselves do not have to specify; it is adapted automatically. For this sector, this represents the convergence of IT and OT.

"Of late, we have developed a far reaching cloud strategy that will eventually be the first choice for all business systems and the transition to cloud delivery of enterprise applications and desktop and mobile services is well underway." [Primary Industry]

4. The application of digital transformation can be used to make the models used for charging and specifying SLAs more sophisticated and more based on 'real time'. Possibly the key disruption that this represents for the MTDC is that it reverses the trend towards cloud. Cloud in different variants becomes one offering among a number.
5. Part of the forward strategy for the MTDC needs to recognise the forward role of edge computing and where the facility will sit in relation to that. This depends upon whether the provider's IoT strategy looks outside the facility across the networks that connect the data center to external data sources.
6. As part of the transformation process, the MTDC will need to organise its personnel and business processes around the process, and it will need also to determine the best partners and suppliers to meet its objectives.

The MTDCs interviewed match the prevailing view from other research – while the opportunity of digital transformation is apparent to all, as is the competitive necessity of embarking on the digital journey, most of these companies are at the start of it.

"We will fit out as demanded with high performance computing in a hyper-converged configuration to allow for data analytics – all those emerging technologies will become main stream." [IT Services] ▶

▶ A number of factors are holding back progress:

1. The age and specification of the facility. Particularly for facilities built in the legacy era to offer space, racks, power and security, there is concern as to whether the data center can be upgraded to meet the requirements of digital transformation and still offer a reasonable return on investment..
2. There is uncertainty as to how enterprise and IT services demand will pan out as a result of digital transformation, and therefore how far the MTDC provider should depart from existing business and delivery models. The MTDC sector is one where clients play an uncertain role:

"Some know exactly what they want, others have no idea – they come to you with a problem they want solve and ask you to solve it. The IT and cloud [service] people tend to know, the enterprise less so". [IT Services]

3. Since the data center – one of the keys to the whole process of digital transformation – is also the key to the MTDC business (it is what they are selling), this may create a Catch-22 situation whereby the provider organisation (which usually keeps an area in its own data centers for its own IT) will not digitize its own practices out of step with the overall data center.
4. Most data center dependent organisations are still organised into silos particularly those that separate the management of IT from the management of facilities and this may impede the development of a unified technological change process. ●

The Internet of Things & the MTDC

"In a few decades' time, computers will be interwoven into almost every industrial product". [Karl Steinbuch, 1966]
Dealing with IoT and capitalising on the opportunities it presents is a core element of digital transformation. As a subset of 'big data', it is far more important than humans as a source of data traffic. It is estimated that by 2020 there will be 50 Zettabytes of data generated by more than 25 billion connected devices.

This represents an opportunity for MTDCs, since it offers insight that can transform the way employees, suppliers, customers, products and processes are understood and how facilities are designed and operated. However, companies mention that they have struggled to understand and communicate the benefits IoT can generate for their data center and determine how to deploy a strategy. The perception that digital transformation is unmanageably large and imposing can be linked directly to perceptions and experience of IoT.

IoT is a key part of digital transformation. For the MTDC it will extend the knowledge of and interaction with clients and lead to more effective decision making in relation to them. It will also facilitate that process in relation to external links into the data center such as networks and other components of a client's data infrastructure if the MTDC is to act as the core control point of that infrastructure. This role will take on an added importance if the MTDC is to operate within a core-edge computing configuration.

The situations in which IoT can be of greatest value to the data center will reflect the previously stated transformation strategy and include operations, CRM, business development, infrastructure utilization, virtualization, capacity planning, operating systems and data products. Depending on the business opportunity to be realised, an MTDC may need to implement a number of IoT technologies and strategies.

All of the characteristics of the huge growth in IoT data will put pressure on the processing, storage and analysis capabilities of the MTDC:

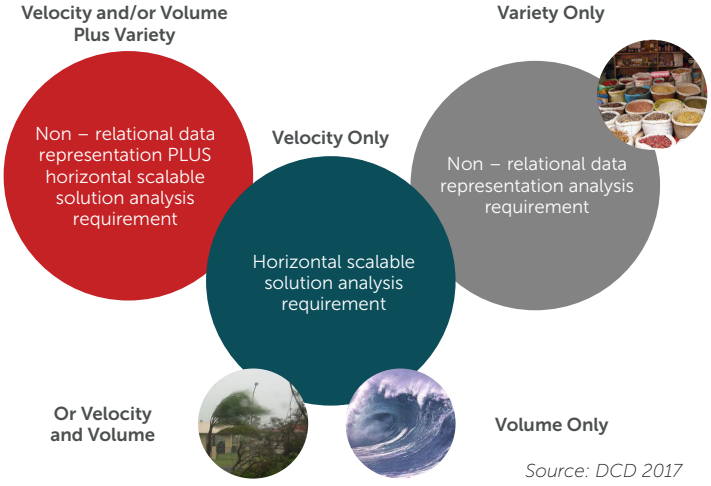
- Big data - the phenomenon of which IoT is the major contributor - is described in terms of:
- Volume refers to the amount of data generated. A decade ago, data storage for analytics was counted in terabytes. Now, organisations require at least petabytes of storage and the data capacity of larger MTDCs may be measured in zettabytes.
- Velocity refers to both the throughput of data and its latency. The legacy era was characterised by regularly batching data, now access and processing occurs in real time measured in terms of gigabytes or terabytes per second. Latency relates to the delay between the data ingestion and the data analysis (measured in terms of milliseconds).
- Variety refers to both the number of data sources and the heterogeneity of data (structured, semi structured or unstructured). Traditional analysis has dealt usually with homogeneous data sources. Variability is a factor in this – this is the phenomenon whereby data units can constantly change meaning therefore requiring a variable analysis framework.
- Veracity means ensuring that the data is accurate and that data that does not conform to the standards required of accuracy does not accumulate in systems.
- Visualisation is important since a clear window on the data makes it easier to validate and use for decision making.
- Value is the objective of the IoT analysis process and just as other projects and processes are subject to ROI criteria so should this process be.

Since the format and structure of IoT data can be established in advance, the issues of variety, variability and veracity may have less impact than for human sources of data. Nevertheless, IoT data from a number of different sources may need consistent protocol and language to be included within the same analytic processes. This is one of the key challenges facing the development of edge processing.

The deployment of IoT will require:

- Sensors at the point where data is collected,
- Sensor technology to manage and direct the sensors,
- RFID tags,
- Embedded systems technology to direct the data flow,
- The means of analysis of the data through IoT analytics,
- The means of acting on the findings through human intervention and/or AI, machine learning or cognitive solutions. ▶

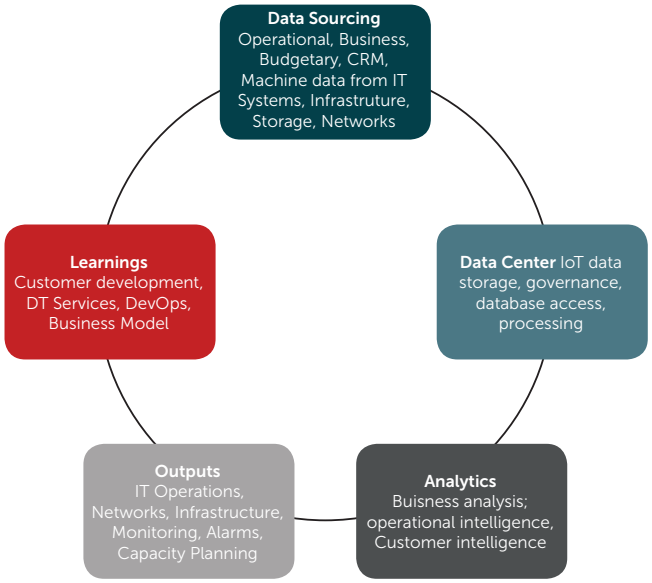
Figure 9: The Classification and Analysis Requirements of Big Data



Source: DCD 2017

▶ The National Institute of Standards and Technology (NIST) suggests that companies consider two crucial data typologies when defining the methodology for working IoT: non-relational data representation, that is when data is semi-structured rather than fully structured and tabular, and horizontal scalability which is valuable when the amount of data coming in increases very quickly since the data on one particular subject (a user or a device) is held in one place rather than being spread across multiple structured tables and therefore separated across servers. This allows for better control over availability, speed and cost. However, this method makes it difficult to enforce relationships between records and therefore to preserve data integrity. Ultimately, therefore the decision needs to be related back to corporate priorities for the data and the need to preserve data relationships. While the choice of non-relational data representation and scalability may be an obvious decision for high-volume, simple and real-time analytics, in the situation within an MTDC where different data sets (operational and CRM, for example) need to be related to provide necessary value, then the decision may not be so obvious.

Figure 10: A Model for the Deployment of IoT Technologies in MTDCs



Source: DCD 2017

This provides a comprehensive understanding of the different big data scenarios that can be found in an organisation. Within an organisation, different types of IoT data can be found, depending on the business problem to be solved, which means that an organisation might need to implement multiple big data technologies.

The need to capture, process, store and analyse data to generate corporate value has generated the emergence of a new breed of technologies. Critical to the process of using IoT are two main categories of technology – for storage given the huge amount of data involved, and processing. Under the first category come NoSQL data stores, Apache Hadoop, Microsoft HDInsight, in-memory databases and distributed file systems. Under the second are Massive Parallel Processing (MPP), Hive, Big data in Excel. These two sets of technologies work in pairs to store and process, sometimes with a third access technology such as Polybase, Presto and Sqoop.

IoT will play a critical component of more companies in future as organisations seek to monitor and optimise the data lifecycle. Efficient use of IoT in this context requires the data source to be defined. All elements of the MTDC may be relevant data sources to examine. Each of them provides valuable information for understanding the performance of infrastructure and enables infrastructure to be optimised. Ultimately, machine and software data is the key to unlocking analytic applications. Analysis conducted by DCD in 2016 [Cavanagh] indicates a number of areas of infrastructure worthy of particular attention:

- **Power** – Elements of the power infrastructure are the electrical service entrances of buildings, the main distribution unit, generators, uninterruptible power supply (UPS) systems and batteries, surge protection, transformers, distribution panels and circuit breakers.
- **Cooling** – Systems that remove heat from the data center include computerroom air-conditioning units (CRACs) and their associated subsystems, chillers, cooling towers, condensers, pump packages, piping, and rack- or row-level cooling or air-distribution devices.
- **Cabling** – Data cables use different materials and connectors to optimise performance and flexibility, while the efficient management of the system maintains this optimisation for the long haul.
- **Racks and physical structure** – The most critical of these elements are the racks, which house IT equipment; physical-room elements, such as dropped ceilings and raised floors; and pathways to manage cabling.
- **Facility management** – Provide visibility of all physical components. Management systems include building-management systems, network management systems, data center infrastructure management software and other monitoring hardware and software.
- **Grounding** – This covers the common bonding network and ground gear that protect equipment from electrostatic discharge.
- **Security and fire protection** – Subsystems included here are physical security devices at the room and rack level and fire-detection or suppression systems. ▶

▶In addition to the operational deployment of IoT, since the data center is the source of business rather than just the enabler and the clients are inside the facility rather than outside, so the IoT needs to be related back to individual customer, budgetary and contractual objectives. An overall model for IoT deployment would therefore build in the following elements:

The IoT platform should operate in conjunction with the enterprise cloud and analysis platforms as a key to the orchestration of its complex eco-system. ●

Analytics

Analytics is the exhaustive use of data, statistical and quantitative analysis, explanatory and predictive models, and data-driven management to drive decisions and actions. Analytics can be the input used for human decision-making or it may drive fully automated decisions. In short, analytics enables decision-making based on data and evidence, rather than speculation and 'hunch'. Analytics is important because data on its own is simply a set of numbers (or other measurement units). Data itself needs to be transformed to be able to be useful. The most usual spectrum to describe this process moves from data through to wisdom as the level of understanding progresses:

Figure 11: The Data Assimilation Spectrum

Source: DCD 2017

There are many benefits of deploying analytics for IoT within the data center. These are linked with the reasons for deploying IoT since analytics forms the processing component of the data generated by IoT. The benefits can be described in terms of the evolution of strategy through different types of analysis:

- Descriptive analysis – The MTDC provider is able to measure what happened in the data center. For example, such analysis can show how much electricity the data center has used over the past week. This enables the provider to gain operational visibility across data center infrastructure.
- Diagnostic analysis – The organisation is able to understand why certain events happen in its data center – such as why the data center consumed more power last week than this. Events can then be linked to causes. Causality enables strategies to be developed on the basis of being able to influence events.
- Predictive analysis – The organisation is able to predict certain data center interactions – namely, how much data center energy a particular client will need or what the impact will be of raising the temperature at which the IT is run by 1°C. This requires more complex analysis and usually some form of statistical modelling to establish how monitoring infrastructure in real time and correlating events across layers leads to certain outcomes, and with what degree of certainty these outcomes happen. These processes apply also to the next two forms of analysis.
- Prescriptive analysis – The organisation is able to make decisions related to its data center based on scenarios. For example, it can identify data-center energy optimisation strategies.
- Preventive analysis – The organisation is able to act in advance of data center needs, such as increasing data center capabilities based on a public cloud.

It is worth noting that MTDCs need a structured, actionable path toward optimising their facilities in terms of business objectives by leveraging data and analytics for their decision-making.

Developing a data center analytics strategy involves an evolution through different stages that include description, diagnostics, prediction, prescriptive analysis and prevention. In addition to helping MTDCs to find solutions to practical operational problems, analytics in the data center opens the door to new data-driven opportunities in terms of CRM and service development.

The deployment of IoT analytics will entail a number of significant process issues that need to be overcome including data generation, data quality, data capture, processing and storage, IoT focus and the availability of both required capabilities and integration skills. The development of analytics needs to be based on a longer-term strategic view and through a process which allows learnings to be incorporated with flexibility into the direction. There needs also to be a cultural change whereby intuition and hunch move towards data-based decision making.

It will have also HR implications. MTDCs have, historically, put a greater focus on the facility than on IT but their IT departments will also need more employees, not fewer, and they will need to look also at employing the new breed of experts in terms of Data Science/Analytics, DevOps and CRM. These are skills sets now in considerable demand. In HR terms, the process will erode the value of the facility and IT silos, and require the redefinition of roles based on workloads and objectives.

"Typically on-prem is reserved for the most sensitive of data – much of our systems that we manage are client owned, we treat these are part of our internal systems in terms of the way we govern their operation – it is highly complex some on-prem is owned and operated by us and then we have cloud services – some of which are contractually owned by clients and some by us and simply resold. Across each service model we have varied delivery methods – we tend to have a dedicated IT team for each contract and for each major location. We have a strengthening affinity with cloud delivery and seek to deliver cost savings not only for our own ▶

▶*business but also for clients by ensuring we maximise the use of cloud systems that have proven to reduce costs and maintain high service availability".* [Financial Services]

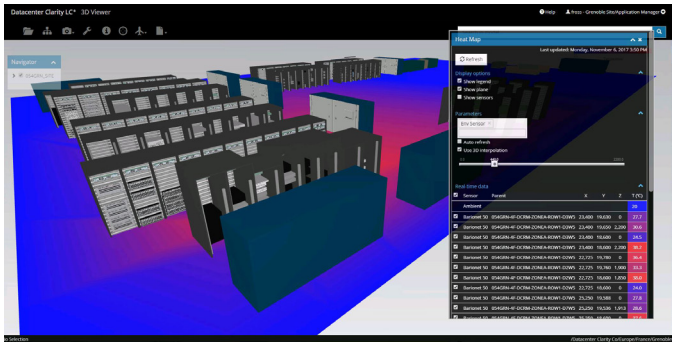
The scarcity of data related to the data center will no longer be the characteristic that defines MTDC provider's efforts to understand their data centers. Increasingly the issue will be how to define what constitutes useful information. It is estimated that by 2020 there will be more than 200 billion sensors across more than 300 billion terminals, each producing an average of 25 exabytes of data per month.

There are significant issues that accompany the deployment of analytics and which determine its use in future decision making, whether human or AI-based. These include issues of:

- **Data generation:** To deploy these big data/IoT initiatives, organisations must first generate data. Although this might seem unlikely, not all MTDCs generate sufficient quantities of data related to their data centers to make IoT analytics viable.
- **Data quality:** Decision-making requires data of a reliable quality. Machines generate the virtually all the data in the MTDC scenario, reducing potential quality problems. However to ensure this, particularly in a situation of increased cyber-vulnerability, analyses to validate data health should be deployed.
- **Data curation:** The potentially huge amounts of data that an IoT initiative will generate needs curation – the process whereby what is useful is distinguished from what is not. Without this step of the process, the data generated runs the risk of flooding the networks, processing and storage systems or at the least using considerable resources unnecessarily. This is a core principle of edge computing – that if processing can be done at the point where data is collected or at nodes before the central processing activity, then this reduces otherwise unmanageable amounts of data.
- **Data capture, processing and storage:** Depending on the requirements of horizontal scalability and relational limitation and the nature of their data, companies will generate a specific IoT type that will require the selection of appropriate big data technology for storage, access and processing.
- **Data focus:** The MTDC needs to focus on areas perceived to have the greatest impact on its business. Again, the wide net that can be cast using big data analysis technology means that the perceptions can be tested to ensure they remain correct.
- **Lack of capabilities and integration skills:** The majority of MTDC providers don't have a team of experts on big data and analytics, and during the initial phase they may rely on third parties to overcome this skills shortage.

The learnings from IoT analytics will transform an MTDC provider, from the management team to the data center infrastructure. The process of becoming a data-driven organisation requires a complete transformation that affects culture, capabilities, processes and infrastructure. It is not limited to the data center even for a company whose business is based on the data center.
The appetite for more knowledge about big data and analytics has steadily increased year by year, as the emergence of thousands of big-data education programs shows. As a result, many companies have deployed big data analytics initiatives related to marketing, finance and operations, and the number of use cases are growing. Working in a broader big data analytic strategy that includes the data center will become increasingly important for all companies and act as a source of business for the MTDC provider. ●

Figure 12: Sensors monitor rack temperature distribution which is then depicted as a real time heat map.



Source: Siemens, 2017

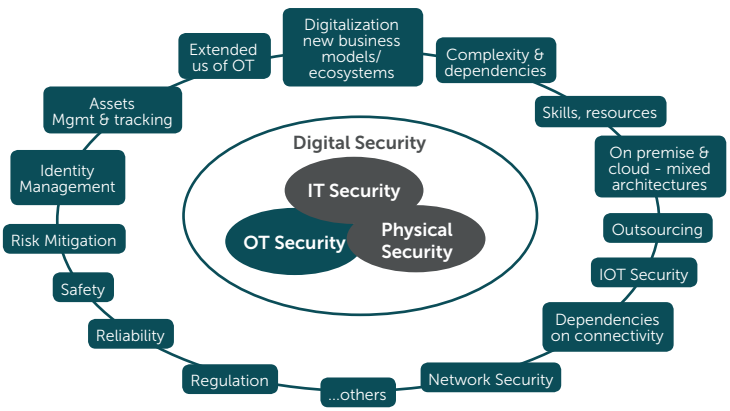
Security

Introduction

Breaches of data center security are reported regularly in the media although these breaches are likely to be only the tip of the iceberg as companies are reluctant to publicise failures. Those reported indicate that the financial costs of disruption can be considerable. The CEO of British Airways put the cost of a power outage that led to the cancellation of hundreds of flights in May 2017 at around BDP 80 million (around USD 100 million). The July 2015 suspension of trading on the New York Stock Exchange for three and a half hours cut the number of shares traded from a 'usual' 600 to 700 million down to 444 million. The Ponemon Institute/IBM Security study estimated in 2017 that the average cost of a data breach among a sample of 419 companies was USD 3.62 million. It estimated also that the probability of a breach over the next 24 months was 28% for these organisations.

In addition to loss of revenue, the cost of a security breach to an organisation can encompass the costs of repairing and upgrading systems, of customer notification and the settlement of legal action. In the case of MTDCs there may be legal action if the breach breaks the SLA and contract between the provider and the client. The loss of reputation and brand can be incalculable, while the loss of market valuation can be highly damaging. Data breach may also result in heavy financial penalties – non-compliance with the EU's General Data Protection Regulation can lead to fines of up to 20 million euros (around USD 24 million) or 4% of global annual turnover. Simple math suggests that this may, in worst case scenarios, mean a shrinking company or closure.

Figure 13: The Security Landscape



Source: Siemens 2017

Attention to security underpins everything that an organisation does across its IT and operational activities.

The provision of digital, information and physical security measures by the MTDC providers needs to meet new threats which are continually striving to outflank the means of protection and which may gain greater traction through the increased IT dependence that digital transformation brings. For the MTDC, the data center is not an enabler, it is the business core and therefore there is an added factor. Security provision cannot compromise the agility of the data center through sheer weight of capacity requirement. Therefore the thinking behind the security requirements of the new digital era needs to change from one that is based on the all-out protection of a barrier to one that is more strategic and based on intelligent technology. ●

The Threat Environment

The operators of MTDCs are faced with the tasks of securing growing and evolving network architectures against increasingly sophisticated and targeted attacks, while at the same time meeting ever more stringent compliance and regulatory requirements to protect the data with which they are entrusted. The most common current security threats on the cyber level faced include:

- DDoS attacks – which have increased since the rise of botnets and have moved the scope of attack from PCs to servers. DDoS attacks are increasingly launched in conjunction with SSL-induced security 'blind spots'.
- Web Application attacks such as SQL injection and cross-site scripting.
- Brute Force Attack - A basic attack method in which the attacker tries to gain access to a website by repeatedly trying usernames and passwords. This may cause disruption as large numbers of repeated requests may tie up memory and processing capacity.
- Ransomware (where data is held for ransom supposedly until a ransom is paid).
- DNS Infrastructure Attacks which have the capacity to disrupt users accessing Internet services and which have occasionally led to class actions against the ISP
- Malware (code directed with malicious intent to steal data or incapacitate computing equipment) including Trojans, viruses and worms. This has now morphed into malware that can act across platforms.
- XSS - Cross-site scripting: a security vulnerability typically found in web applications which enables an attacker to inject client-side script into web pages viewed by other users and can be used by attackers to bypass access controls.
- Man-in-the-middle attack - a network attack whereby the attacker secretly relays and possibly alters the communication between two parties who believe they are communicating directly with each other.
- Phishing (illegitimate requests for information and passwords).
- Unpatched software, most commonly browser add-in programs.
- APT - Advanced persistent threat: a network attack in which an unauthorized entity gains access to a network and stays undetected for a long period.
- Social media threats
- Advanced persistent threats (APTs) via (spear) phishing

Just like natural viruses which mutate in order to survive against antibiotics, so the list above will mutate and combine in order to present a more sustained and complex mode of attack.

The New Security Focus

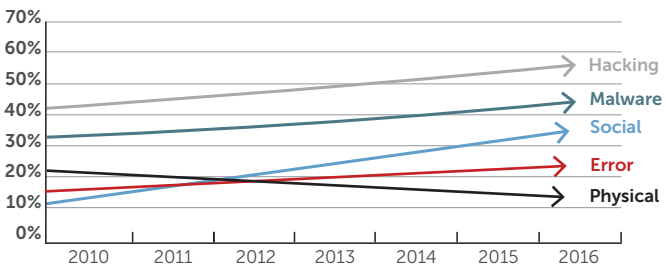
The protection of the environments in an MTDC that are and will be created as digitalization evolves will differ from the requirements of protecting a legacy data center.

There are therefore a number of important considerations for developing a security model in an MTDC:

- It needs to reflect the changing design and operation of a multi-tenant facility and be designed for the mix of services and environment offered by the facility (or facilities). While the principles of security are general so their application to each facility in terms of IT protection, OT protection and physical measures will be different. There is no 'one size fits all'.
- The measures taken must be able to adapt so that they provides consistent, constant and intelligent protection across evolving and hybrid data center models.
- They need to provide protection against advanced and evolving threats.
- They will only be as strong as their weakest link therefore they needs to observe principles of protection that use multiple levels and back up, described variously as 'end to end', 'layered' or 'zero trust' depending on the form of security.

While the focus of security has moved to cyber-threats based on the changing profile of the data infrastructure landscape, other sources of disruption should not be ignored. Hacking, malware and threats delivered via social media have grown the most to 2015 in terms of numbers while physical, environmental and disruptions caused by error and 'misuse' have remained at a consistent level. This cluster of threats remain at a level however where they cannot be ignored.

Figure 14: Growth of Threats to 2015 as % of All (Representational only)



Source: Representational from Verizon

Traditional approaches to network security were based on the principle of an environment at the edge of the internet which could be protected at the perimeter and not for environments that incorporate a 'hybrid' and virtualized mix of devices, data centers, clouds and applications. Traditional security approaches are inadequate against the level of cyber security threat coming across the evolving network. Of particular note is the threat posed by attacks which sit 'live' within the perimeter for an average of more than 200 days before being detected.

Figure 15: Comparison of Security Requirements between a Traditional and a Digitalized Environment

Security Requirement	Traditional	Digitalized
Overall Intention	Prevention & diagnosis	'Real time' threat management, isolation and elimination
Focus	Securing the perimeter to protect established internal network	Securing applications and data inside network, protection of lateral spread of attacks if perimeter is breached
Adaptability of Threat Response	Pre-defined	Automatic
Visibility of End Points	Little/none	Real time, continuous monitoring and diagnostics
Detection	Signature-based malware	As above using IoT analytics
Integration	Limited	Sharing of information
Threat Response	Slower	Immediate/'live'
Provisioning	Can be lengthy	Immediate/as needed
Scalability	Limited	As needed
Establishment	Tied to physical devices, signature-based, firewalls, IPS, anti-virus software, VLANs and server zones. Policies need to be changed by human intervention item by item.	Delivered digitally, instant updates and policy changes. Evolving use of IoT + AI to automate this process.

The cybersecurity risk to the service data center is accentuated by the dependence on virtualisation, cloud computing and the internet of things (IoT). One of the major opportunities presented by digitalization within the MTDC environment is for the intelligent automated management and control of data center OT. In line with the ultimate focus of digitalization on customer delivery, this will enable better provisioning, customization of services and more user-based charging models.

In terms of both IT and OT, server virtualisation allows more efficient management and control of workloads. Software defined networking (SDN) offers the same benefit for the network via application programming interfaces (APIs). Infrastructure as a service (IaaS) enables easy provisioning and deployment of servers and applications, while organisations embrace software as a service (SaaS) in the cloud:

"The biggest trend we are seeing is the ability to move services to SaaS delivery and this is typically our first option for a lot of small systems deployment for specialist roles. We have moved email and collaboration to SaaS delivery as this is more readily accessible to more of our workforce." [IT Services] ▶

▶ All of these technologies and environments are mentioned as part of the process of MTDC digital transformation and they therefore will be deployed across the multi-tenant data infrastructure portfolio.

This creates the potential for greater vulnerabilities across the network as it presents more opportunities for attackers to compromise a facility as its increased complexity and dispersion creates a far wider attack surface. Data from IoT presents another challenge as data must be protected by access controls and monitored on a real-time basis in a situation where it may be difficult to ensure the security of the end points and of the mission-critical information that is stored within the IoT data set. There will be a huge number of such endpoints within even a single data center and their interconnection – the network foundation of the IoT – will lead to a more complex and disparate network architecture. As the equipment within the MTDC becomes integrated, so the online threat to the security of physical infrastructure begins to take a shape parallel to the cyber-threats against the IT housed in the facility. The deployment of the internet of things (IoT) will create a vast array of endpoints even within a single multi-tenant data center. The interconnection of these objects will result in exponentially more disparate and complex network and fabric architectures.

It now widely accepted that security must be deployed throughout an organisation's whole data infrastructure, and out to the growing number of endpoints that are connected to that infrastructure. This needs to offer greater visibility into the network. Ideally, the role of the MTDC within a wider data infrastructure needs to enable the use of one set of security capabilities running across different the different data infrastructure environments - public cloud, private cloud, within the MTDC and within other on-prem or outsourced environments. A large number of security protocols and administrations are complex to manage, and this may restrict visibility and control across the entire portfolio. This is important as one of the most major consequences of digital transformation is the growth in hybrid environments, multi-cloud and flexible provisioning. ●

Assessing the Threat and Reducing the Attack Surface

Protection of the next-generation MTDC needs to work from the basis of securing the network and with that, all that connected to it. More than the traditional approaches, the MTDC provider needs now to understand the security risks against the facility and then implement specific measures to reduce or minimise unacceptable levels of risk. This might include reducing the severity of the consequences of an attack, reduce the probability of an attack occurring, or reducing exposure to the attack.
The first priority is to reduce the 'attack surface', that is the various places or vectors at which an unauthorised user or attacker could get into a system or get data out. The 'attack surface' needs to be looked at in terms of the network layer, the software layer (with a particular focus on web applications) and the human/user layer. There are many sources that indicate the user as the weakest line of defense. This is true particularly of MTDCs where access needs to be provided to clients on both a physical and cyber level and which may therefore present duplicative attack surfaces.

The process of reducing the attack surface follows the inherent security principle of keeping out threats while permitting authorized access. This is most effective when using a least trust approach – reducing the exposure of system targets, protecting the network and getting visibility segment by segment, being stringent in the issuing and enforcement of authorization and reducing where possible the amount of data that needs to be processed or transmitted by deploying software and procedures including that of data curation which can be used to restrict the amount of data vulnerable at an attack surface. Preliminary measure will include:

1. Traffic segmentation as a means of filtering, analysing and verifying network activity. This will reduce the potential attack surface through introducing protections such as firewalls and switch access control lists. Segmentation of a network can make it easier to isolate and analyse traffic patterns and as an aid to visibility but it is not per se proactive in enforcing authorisation or the control of privileged information or inspecting traffic for threats.

2. Identifying the data and applications that need protection. This means that an MTDC provider must gain visibility across their entire network and everything on it, without compromising the day to-day operation of the business. The transaction flows for these applications must also be mapped so that segmentation gateways can be deployed as appropriate and with the right application, user and content policies.

3. Security must work across the multi-tenant data center so that clients, both internal and external to the hosting organisations can rest assured that their data and applications are safe. This means a consistent and accurate security policy across heterogeneous environments.

4. Advanced endpoint security solutions must be considered a priority given the number of different IoT endpoints connected to the network(s) within the MTDC, the vulnerability of these and the mission critical nature of the equipment and systems operated using the data generated.

5. Underlying and overlapping these measures is the need for intelligent security, that can identify and block attacks in real time, and then use the knowledge to inform and prevent future attacks.

6. Applications, and even workloads within applications, can be segmented using a network-based approach. ●

Software-Defined Security & The Role of Analytics

Cyber-security has always been, by definition, software-based. It include any type of software that secures and protects any network or computing device from the range of viruses, malware, unauthorised access attempts and other security vulnerabilities listed earlier in this chapter.

While IoT within the data center can collect data through which problems and threats can be identified, the defense against cyber-threats increasingly takes the form of analytics that can identify statistical abnormalities, trace the cause and put necessary responses into place. This approach will increasingly be adopted by MTDCs given the increased security risk represented by multiple clients and their IT within a common space and, sometimes, network as well.

The development of software-defined networking (SDN) particularly and to an increasingly lesser degree network functions virtualisation (NFV) is the logical progression of software definition which has been used for the definition of networks and other elements of data center infrastructure through APIs, into security. The programmability and automation inherent in software definition can be used also in security to deliver a more agile and responsive system as well as offering the key benefit of a centralized control engine with a high degree of orchestration which allows for incisive analysis and swift response to threats.

Once the principles of software definition are applied to security it allows key steps in the security process to be automated and monitored such as detection and prevention of threat or intrusion, network segmentation, monitoring and access controls. The security control plane is separated through these protocols from the security processing and forwarding planes.

It also allows the automatic inclusion and control of any new device under the appropriate security policy and protocols. This includes applications and workloads within applications created within the IT environment (usually cloud or virtualised infrastructure) regardless of where the device is located. The device can also be migrated, moved within the data center or scaled and the security policy and controls remain with it. This is of particular value within an MTDC as it will reduce the time and trouble of re-allocating security protocols when tenants take or reduce footprint or move in or out. It obviously reduces the possibility of human error and the time spent in re-defining protocol.

Software-Defined Security is adaptive in that the security policy and controls automatically remain with the device if is moved, migrated or scaled, which speeds up response time and reduces the scope for human error.

While the fast, intelligent identification of and response to threats is a key attribute, it may not in itself be enough. A number of threats base their damage potential on sheer volume and the combination of a range of threats and alerts may be too great for a security system to deal with. Therefore, intelligence and analysis that can move beyond the prevention of current attacks towards the detection of potential attacks before they happen is of considerable value.

There are a number of different types of intelligence approaches that can be used to achieve this including threat exposure (vulnerability) management, threat intelligence, enterprise forensics and incident response. An organisation may need to use multiple approaches in order to maximise protection. Machine intelligence and human intelligence both play a role in this process with the former offering the capability of mining and analysing vast amounts of data in real-time and human intelligence acting as the start point for scoping the analytics and the end point in terms of working out what to do with the findings.

Increasingly, sophisticated algorithm-based techniques are used in conjunction with big data analytics, not just to identify security threats but to diagnose the wider principle of 'data health'. A data pattern can be considered as the mathematical expression of specific network behavior developed on the basis of prior empirical learnings. The ability to recognise behaviors in data on this basis has tremendous implications for detecting pre-defined incidents.

Threat intelligence seeks to detect anomalies, by establishing a baseline of normal behavior so that abnormalities can be detected through the use of user behavior and user analytics. It can also look at the tools, techniques and procedures used by attackers from the evidence left behind in an attack. From this intelligence, countermeasures can be implemented to reduce the likelihood and/or the impact of future attacks.

Network Anomaly Detection is the process of finding behaviors in network traffic indicated by the analytic which do not conform to expected patterns. These nonconforming behaviors may indicate a range of possibilities such as impacts on the end user Quality of Experience, degradation of equipment or performance, security and intrusion detection or attack blockers when the anomalies are detected in the network in the early stages. Security measures need therefore the ability to proactively detect network anomalies and detect unknown network behaviors without using any evident signatures, labeled traffic, or learning. It needs to base its detection methodology on its continual refinement of learnings from the data it collects. A possible analogy here is the data methodology behind the autonomous (or 'driverless') car. It will not have met before every single driving situation on every single road that it will travel. Rather it will work from the broad characteristics of situations and ▶

▶outcomes to determine the most suitable reaction - for example, speed, proximity of other vehicles, road and weather conditions, local road rules, physical condition of the vehicle, IT and network health to determine safety outcomes. Where the situation is outside the boundaries of the car's learning it will need to collect more data about the situation and/or transmit it to the core processing unit for analysis and instruction.

In current network systems, by monitoring certain thresholds, warnings and alarms are triggered to indicate an incident in the network. These can then be investigated manually starting with the most critical ones. This requires comprehensive knowledge about the network architecture, its elements, and their capabilities. It is more effective to use an approach based on measuring distances between any individual entity (such as a cell, or a KPI) and behaviors either previously identified and labeled as abnormal, or automatically learnt as a deviation from the normal expected behavior. This method avoids long post-mortem investigation times. Root Cause Isolation Root Cause Isolation (RCI) is the process of identifying the source of anomalies and therefore of possible threats in a system on the basis only of data observation. Many OSS systems and NOCs suffer from a common problem: when the network fails to function correctly, it is often difficult to determine which part is the source of the problem.

The fundamental challenge is that the symptoms of a failure often manifest as end-to-end failures in the operation of the system, without causing obvious initial failures in the system/ cell components, thus compromising its predictive value. In general, cell outage takes place due to multiple reasons, such as hardware or software failures including misconfigurations or bugs or even changes to the environment. Usually, the detection of a malfunctioning cell is performed through the analysis of alarms, KPIs, or in many cases, multiple customer complaints.

Cell malfunction can be classified in a number of ways – from reduced functionality, through degraded performance, to complete inoperability. The initial, least serious form of cell malfunction has traditionally been invisible for network operators through traditional alarms. This peculiarity makes its detection a very challenging task.

Root-Cause analysis involves an automatic investigation of problem KPIs and diagnosis regarding failure reasons through an automated analytic and diagnosis process. Not every indicator of compromise turns out to be an attack, and the challenge for threat intelligence is to reduce the number of false positives to a manageable level and to those that really warrant investigation. ●

The Importance of Physical Security

Much recent attention on data center security has focused on disruption caused by threats to cybersecurity. Yet focusing efforts purely on this source of threat can draw attention away from the threat of physical attacks on, or accidental damage to, premises and equipment.

For the MTDC, the standard of physical security is one of the key criteria by which they are chosen and judged. As these data centers become denser in terms of space and power utilisation, so the costs of a failure will become greater. MTDC have been able to tie hardware capacity more tightly to utilisation and end user provisioning, notably by employing server and storage virtualisation to consolidate the volume of physical hardware deployed. This has improved the bottom line both in terms of reduced wastage and increased revenue. Saved space has therefore quickly filled with more hardware as MTDCs look to maximise their capacity.

Yet the MTDC set-up put more pressure on physical security requirements, especially in multi-tenant facilities that see many different service providers and their customers house equipment side by side.

Multi-tenant facilities give clients agreed levels of freedom to manage their own software and hardware in a controlled environment, possibly sharing access to server rooms to carry out upgrades, repairs, new installations, and routine maintenance. That increases the volume of traffic, vehicle and human, travelling in and out of the facility. This has the possibility of increasing the threat of disruption if not carefully and securely managed.

The development of a strategy for physical security will not be the same for all MTDCs. An organisation building a new 'greenfield' data center will have considerably greater latitude to follow all the recommended build and design principles and to install all the latest access and anti-intrusion technologies than an organisation hosting its IT in an older facility or as a section in buildings where other commercial, administrative or industrial activity takes place.

There are two related principles that apply to the physical protection of the data center. The first is 'defense in depth', that is to ensure protection is backed up so that if it fails at one point then there is a further defense behind that, and 'layered' security. As data centers need to provide access as well as defense, a key component of security is the need to organise it around a series of points at which further access is allowed or denied to someone seeking entry to the facility.

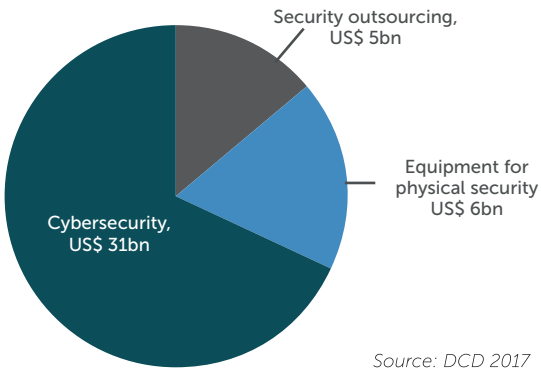
There will be the continuing need to deploy available security measures to protect the data center.

In terms of protection against threats from the areas around the data center this may include building perimeter walls, embankments and fences, multiple security checkpoints, manned security stations, mantraps, biometric readers., locating the building away from the perimeter of the site, keeping equipment racks away from any external walls and away from windows and establishing surveillance networks covering both internal and external areas and perimeters.

Within the data center white space security can be provided by intruder/fire alarm and control systems, lockable racks and cages in multi-tenanted environments, fire-proofed/air-locked doors, powder fire extinguishers, a gas based building wide fire suppression systems and access controls.

Further advances based on facial or retinal recognition, the deployment of AI to drive access and security systems, technological improvements around CCTV, motion detection, the remote control of locking mechanisms, the use of laser technologies to create beams that provide a barrier to a protected zone can be deployed as they are developed.

Figure 16: Estimated value of security investments in MTDC sector 2016 (US billion)



Source: DCD 2017

The analysis of the threats and situations that threaten a data center indicates that, short of catastrophe (usually from natural or human causes), it usually takes more than a single event to cause unplanned downtime. More usually it requires a sequence of events rolling out from an initial cause and these will include the failure of the systems designed to protect against the initial error. Humans usually have a role somewhere – mostly accidentally. Therefore it is critical to establish any shortcomings in the people working or coming into a mission critical facility.

As with commercial airliners, most unplanned downtime occurs as the result of a sequence of events with the start cause as a loss of mains power whether caused by a natural event or grid failure with its run-thru effect on power systems, this is normally followed by failure of back-up power/UPS systems and/or the failure of monitoring/alarm systems and the irrecoverable failure of servers. A similar pattern plays out with the failure of cooling, the occurrence of a thermal event and the loss of availability (and sometimes, worse). One of the key causes of disruption is the over-running of scheduled downtime where no physical damage is done to the data center but disruption is extended. ●

The Siemens Point of View

The research and analysis in the Paper raise some important and complex issues raised by preparing an organisation for digitalisation. With this in mind, DCD spoke with Urs Iten, Director of Global Portfolio Management Data Centers at Siemens about some of these issues.

DCD: How do you read the preparedness of the MTDC companies you are in contact with for digital transformation? The view from the companies we talked to was mixed - interest in the possibility of better business performance through transformation but concern about the sheer scope of the task - does this concur with what you are finding?

Urs Iten, Global Portfolio Manager Data Centers: The data center market still seems to be a relative conservative market. This results ultimately from the major pressure to maintain uptime requirements for such critical infrastructure. Many organizations are not yet fully committed to changing things – there's a sense of "if it ain't broke, don't try to fix it". Indeed, every change creates the potential for additional risk, but it also can generate benefits. This applies also for many situations in our life in general and means that appropriate risk mitigation strategies need to be developed.

We have nowadays access to solutions and technologies through which we can connect almost everything centrally via related applications so we can monitor and control complete data center facility infrastructures remotely, or even go further to automate parts and processes remotely also. Nevertheless, many organizations and their staff do prefer to run their sites in the traditional way. This means that systems and components are not connected to any supervisory tool.

One of the possible downsides of pursuing digital transformation is definitely the requirement for cyber security. As more and more devices are connected on an IP basis this represents potential vulnerabilities. This is something that therefore needs to be considered and managed through the process of digital transformation too.

The principle here is that additional risks need to be accepted and managed in order to reach and generate value-add.

DCD: What do you find are the biggest challenges to the companies you deal with in terms of realizing digital transformation?

Urs Iten, Global Portfolio Manager Data Centers: Basically, everything in life it needs a motivation to change or to unlock the potential for going new and different ways. In the context of digital transformation the added value that can be gained from a new or adjusted business model is the fundamental motivation and starting point. Digital transformation is not for free and it requires investment to prepare the digital platform for example. Beside the platform, the transformation of the organization itself is a key part of the digital transformation of business. Inevitably, people are changing slower than are machines.

In many cases, companies are not yet prepared to consider processes from an end-to-end perspective. Distributed responsibilities across the organisation make it even more challenging.

I'd conclude that the business case together with associated added value is the key element, as well as the transformation of the organization itself and its culture. Decisions therefore have to taken by management from the top down.

The whole process needs to be consider holistically in order to direct specific implement strategies and a step by step approach!

DCD: Just as transformation will change the MTDC data center so it will change also the relationship with the companies that 'supply' into that provider. How do you observe this impacting Siemens? How will this change the way you yourselves do business?

Urs Iten, Global Portfolio Manager Data Centers: Digital transformation also implies that all business partners need to be considered and included into the big picture of the analysis. It also needs to be integrated in terms of the specific implementation of digital business models, with all the associated collaboration that is required.

We are already seeing ourselves as part of such collaboration models, especially in the context of our wide range of service offerings across the life cycle for data centers in many areas of operation such as energy services and in many regions.

DCD: Is best practice possible with digital transformation? Or is the process too new and uncharted?

Urs Iten, Global Portfolio Manager Data Centers: Best practice is possible in our point of view, but with limitations. Best practices can be used in the context of general principles and approaches. The details are likely to be different between different business and use cases. Best practices can also be used to shape the process of organizational transformation, in terms of principles, behaviors and cultures that need be changed. The exact methods of achieving this remain mostly unique to each case, especially in an organization which operates across borders which means it includes different cultures within its domain. ▶

▶ Therefore it is certainly possible to apply best practice but only to a certain level of abstraction. Beyond that, it is very much on the basis of an individual organisation.

DCD: What are key components of how Siemens assist companies dealing with digital transformation? What are the steps, questions, principles of engagement that Siemens are able to bring to the process? What are these based on?

Martin Widmer, Global Marketing Manager Data Centers: Siemens helps data centers around the world to take advantage of digital transformation to create an even greater competitive edge. This is achieved by enhancing data center performance through the power of data. Siemens recommends a 4- step approach to achieve this:

1. Define business objectives and KPIs,
2. Connect systems and collect data,
3. Analyze data to create actionable insights, and,
4. Take action and continuously enhance performance.

Our approach is based on optimizing the interplay of people, technology and services.

This includes global expertise in terms of our deep domain know-how, and project management skills and local market understanding. Our 4 regional Digital Service Centers provide above-site support such as remote maintenance and problem diagnosis. At the same time, we have branches across the globe which ensures a local presence and an understanding of the local market and its regulations. Our combination of above-site and on-site support means we can meet our customer's needs more effectively.

The Siemens integrated data center management suite (IDCMS) provides a holistic management approach for reliable and efficient IT and facility data center operation. Navigator - the cloud-based energy and sustainability management platform from Siemens Building Technologies - provides the industry's most comprehensive insights into total energy management and building performance by seamlessly integrating analytic technology and operational expertise. The platform supports a wide range of best-in-class energy, sustainability and operational management services and solutions. ●

Glossary

ACL
Access control lists – the list of permissions attached to an object whereby access is granted or denied.

AI
Artificial intelligence – the demonstration of intelligent behaviour by machines usually on the basis of machine learning.

Analytics
The application of statistics and programming to identify and interpret meaningful patterns in data.

APT
Advanced persistent threats - series of continuous hacking or other cyber threats

BMS
Building management systems – computer based control system to control and manage building's MEP and security systems.

Capacity planning
The advanced anticipation of resource requirements.

Computational Fluid Dynamics
The real time mapping of temperatures within a data center to indicate the risk of thermal events.

CRAC
Computer from air conditioning

CRM
Customer relationship management.

DCIM software
Data center management and control software designed to integrate the operation and planning of both IT and infrastructure stacks.

DDoS attacks
Distributed denial of service attacks which aim to shut down a company's IT services or parts of it.

DevOps
Software engineering that integrates software development and operation.

Digitalization
The process of using technology to change a business model in order to reach new opportunities for revenue and value.

Digital Transformation
The change at a core level of business and organisational activities, culture, processes and models to optimise the opportunities of digital technologies.

Digitisation
The process of transferring analogue data into digital format.

DNS Infrastructure Attacks
Which have the capacity to disrupt users accessing Internet services and which have occasionally led to class actions against the ISP

DR services
Disaster recovery services.

Embedded systems technology
Hybrid IT
The deployment of a number of different environments and systems to store and process data, usually including an on-prem facility or 'legacy' IT options together with cloud services.

IaaS
Infrastructure as a Service which provides virtualised computing resource from a cloud source.

Industry 4.0
The creation of 'smart' manufacturing and production using the digitalization of the process using IT and OT technologies.

IoT
The Internet of Things – the network of devices, appliances and other physical items which are embedded with electronics, sensors, software and actuators and which are networked to connect and exchange data.

ISP
Internet Service Provider.

KPI
Key Performance Indicators, measures of how well a person, team or system is doing.

LBNL
Lawrence Berkeley National Laboratory – a national laboratory in the USA that has researched and published on the issues associated with data center and server energy consumption.

Malware
Malicious software including Trojans, viruses, worms and other forms of hostile or intrusive software.

MTDC
Multi-tenant data center. These are service data centers that share raised-floor space, power and cooling between tenants. They may be shared facilities leased out commercially or data centers run for client groups within a single organisation.

Network (Behaviour) Anomaly Detection
The monitoring of networks for unusual or outlier behavior or trends.

NGFW
Next-generation firewalls.

NIST
The National Institute of Standards and Technology in the United States which focuses on measurement science, standards and technology.

NOC
Network Operations Center.

On-prem data center
A data center run by an organisation to service its own IT requirements. It may also be referred to as a captive, in-house or enterprise data center depending on the organisation.

OSS
Open Source Software.

OT
Operational Technology.

PaaS
Platform as a Service.

Phishing
Illegitimate requests to try and obtain information and passwords.

Ponemon Institute
Institute that conducts independent research on issues of privacy, data protection and data security.

Ransomware
Where data is held for ransom supposedly until a ransom is paid.

RCI
Root Cause Isolation = analysis involves an automatic investigation of problem KPIs and diagnosis regarding failure

RFID tags
Identity and access tags activated by radio frequency.

ROI
Return on Investment.

SaaS
Software as a Service.

SLA
Service Level Agreement.

SME
Small and medium enterprises.

Social media threats
Cyberthreats transmitted via social media.

Software-Defined
Used here in relation to Security (SDS) and Infrastructure (SDI) – technical computing infrastructure controlled by software with no operator or human intervention.

Spear phishing
Electronic scams targeted to specific individuals or organisation usually intended to steal data or install malware.

Utilisation
The metric of how much of an available resource is actually consumed. Used here for IT and power.

Virtual reality
The simulation of a person or device within a computer generated 'virtual' world. Augmented reality may be considered a form of virtual reality as it superimposes layers of virtual information over the experience of either the real or a virtual world.

Virtualization
Digital versions of 'actual' computing, network or storage devices or resources.

VLAN
Virtual local area networks.

VM
Virtual machines – the virtualized equivalent of a 'real' computer.

WAN
Wide Area Networking that extends beyond local or metropolitan networks to cover a large geographic areas.