
DATA CENTRE MICRO-PROTECTION

Analysis of advanced control and protection of physical assets in the cloud



November 2010

1. THE EMERGENCE OF CLOUD COMPUTING AND THE INTERNET OF THINGS

Two technology trends are having a major impact on data centre market developments: the growth of cloud computing services and the evolution of the 'Internet of Things'. These trends present both business opportunities and threats.

CLOUD COMPUTING

The cloud computing 'consumption' service model enables companies to allocate computing power efficiently, on demand, via Web portals, and changes the way computing resources are being used within organisations. New business frameworks are developing for 'IT-as-a-Service', which depend on virtualised servers and automated IT infrastructure. Businesses benefit from improved agility and scalability.

Cloud computing presents new opportunities for businesses and for data centres in terms of

- Ability to focus on core business
- Potential for cost savings
- Use of state of the art IT systems
- Virtual data storage

Companies are better equipped to support their business goals. Companies distinguish between 'core' (critical to the business) and 'contextual' (peripheral to the main business operation). Private or 'internal' clouds are being built by banks, enterprises and governments data centres for critical applications. Non-critical applications such as CRM, accounting, HR, product test and development are hosted on public cloud services either as Software-as-a-Service or Platform-as-a-Service. Data centre operations are being offered as Infrastructure-as-a-Service or as 'Virtual Data Centres'.

The economic recession has accelerated the use of cloud services, data centre co-location and hosted managed service. Cost savings will depend on the level of automation achieved and the type of cloud chosen. Some SMEs, using cloud services in Europe, report cost saving of more than 50 percent.

One of the big advantages of using cloud services is that companies have ready access to state of the art systems without the financial burdens associated with Capex investment. There is increasing use of virtualised technologies and high-powered blade servers in data centres. Cisco reports that 95 percent of their servers shipped are virtualised. The cost benefits and efficiency gains, in terms of server utilisation, power and space are compelling for large organisations with a high number of servers.

Data storage in the cloud is increasingly seen as an attractive option. Typical company storage volumes are forecast to grow from 2 Terabytes in 2010 to 50 Terabytes by 2016. Replication in the cloud will become the norm not only for applications but for entire data centres in order for service providers to deliver 100 percent availability and fail over times of minutes not hours, days or weeks.

THE INTERNET OF THINGS

The Internet is morphing over time from the Internet of People to the Internet of Things, and driving the physical world to behave as an information system in its own right. Demarcation lines between human / IT-centric and machine-centric technologies and systems are blurring. Smart systems, smart business and smart grids are being deployed. Smart systems fall into two groups: IT-centric devices and Machine (non-IT) centric devices. The latter are being implemented on a universal scale with analyst estimates of around 130 million machine-centric devices in place in 2010. This group includes smart networked equipment - intelligent devices such as sensors or appliances such as HVAC systems.

Sensors and actuators are embedded into physical objects which are programmed to sense and communicate. These objects are linked via fixed cable or wireless networks using the Internet Protocol (IP) and will automatically generate detailed data for computer analysis and management reporting. New ways of using and managing smart devices results in increased operational efficiency, higher availability of critical infrastructure and improved safety within a given environment.

Key characteristics of the Internet of Things are:

- System of connected and communicating smart devices
- Delegated intelligence
- Rich data collection
- Remote and peer control
- Self healing capabilities

The Internet of Things introduces new concepts, such as intelligent asset handling and remote asset actuation, into the protection of physical business assets. An early application of the Internet of Things is the use of sensors to track RFID (radio-frequency identification) tags on products for improved inventory and supply chain management. In manufacturing industries, networked sensors are being fitted to vehicles and equipment for early detection of problems and pro-active maintenance.

The Internet of Things and remote actuation (or 'remote hands') has multiple applications across all sectors including IT, fixed and wireless telecoms, transportation, healthcare and medical services, retail, utilities and leisure. In the data centre, it can provide volume data on physical access and environmental conditions both inside and outside a cabinet, cage or rack. This has direct implications for infrastructure availability, energy consumption and costs, as well as health and safety obligations. It also means pro-active management of 'lights out' data centres as well as manned data centres.

The Internet of Things will:

- Track behaviour by monitoring the behaviour of people, things or data through space and in real-time

- Provide companies with enhanced 'situational' awareness of environmental conditions, e.g., overheating within a rack
- Support automation and control processes - analysed data can feed instructions back to remote actuators to adjust temperatures or open/close doors
- Enhance business control, planning and decision-making - the management information generated can be used to support other processes across the business.

MANAGING THE NEW RISKS

Virtualised environments and hosted cloud computing services opens up new business risks for customers. It also places new demands on data centre service providers and operators.

Today, there is a widely held view that data is less secure in the cloud and 'security' threat is a major inhibitor to the adoption of public cloud services by large enterprises, banks and governments. Once 'out there' in the cloud, IT assets are exposed to access by other people and to environments over which customer have no control. Cloud computing means allowing external administrators access, manage and control your business data and both business and legal measures have to be taken to mitigate risks.¹.

Major concerns include:

- Access by other people to the company's assets
- Third party maintenance and control of customer assets
- Environments that could prove harmful
- Failure to comply with regulation

Cloud also raises issues of data protection associated with national and European regulations, the USA's Patriot's Act and sector legislation and compliance. Cloud computing places demanding requirements on both users and service providers' data centres too.

There is increased emphasis on:

- Safer environment
- Stricter rules for access
- Visibility to customers
- Meeting service level agreements (SLAs)
- 'Always on' availability
- High quality managed services

¹ See: Will your move to the cloud open up your company to security threats? *SAPinsider*, Oct.2010

- Increased power consumption and monitoring
- Guaranteed compliance with regulation

DATA CENTRE MODELS AND PHYSICAL PROTECTION

Individual operational models used will affect the level of protection required but all data centres irrespective of ownership, size or location face a common challenge of keeping their IT assets safe in hosted environments where assets are dispersed around the globe.

Data centre facilities vary and there are a number of models in use today:

Carrier neutral - this is the simplest of the data centre offerings focusing on the low-end, retail space, with typically at least five carriers interconnected to them. These specialists are generally not dependent on any one customer for more than 5% of revenues. Global specialists include Equinix, Terremark and pan-European operators like TeleCity and Interxion. A carrier neutral facility may have as many as 400 - 600 customers.

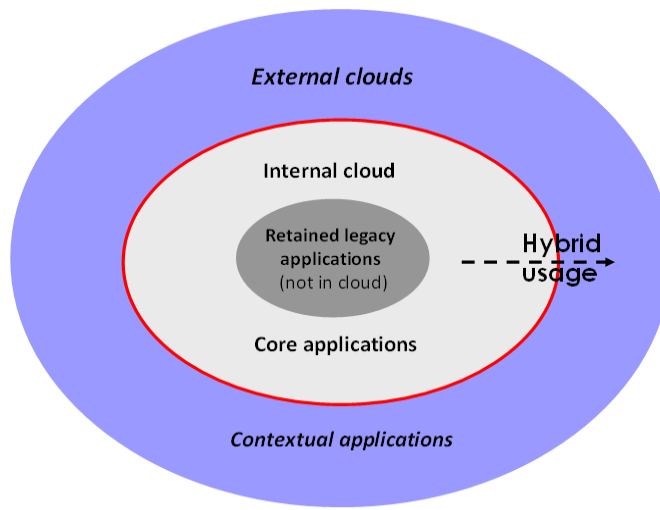
Wholesale - these players typically operate data centres of 10,000ft² or above. Leading players include QTS, Global Switch and Digital Realty Trust (four largest customers globally are Equinix, Savvis, Level 3 and Telx). Client base is comprised of Fortune 500 companies, large enterprises and banks. The wholesale data centre typically houses three or four different tenants, sometimes a single tenant.

Telco co-location and hosting - telcos use their data centres for both their own purposes and external service provision. Leading players include AT&T, BT, COLT Telecom, France Telecom, Verizon, NTT, Telstra, Global Crossing and T-Systems (Deutsche Telekom). Depending on telco, service offerings include: co-location, managed services, outsourcing and hosted cloud services and virtual data centres.

Managed services - covers a wide variety of players offering services such as disaster recovery services (e.g., SunGard), outsourcing (e.g, IBM, HP and owners/tenants) as well as niche managed services specialists and hosters/cloud providers such as Savvis and Rackspace.

Enterprise users - the majority of the data centre market is comprised of in-house facilities run by multi-national corporations, large or medium sized businesses. In the light of the current economic climate, enterprises are evaluating the economics of their purpose-built data centres and there are increasing decisions to outsource to third party operators and use managed service providers. As cloud services evolve, large businesses are transitioning to use a hybrid mix of both in-house and externally sourced cloud services and virtual data centre services.

The next graphic illustrates this hybrid mix:



Enterprise cloud adoption model for the next 5 years
Source: Broadgroup, 2010

Government - has very specific requirements both at the national and local level. There is a move to data centre consolidation at national, state and local government levels, as well as growing interest in cloud computing services. The US Federal Government is promoting cloud services for its citizens. Governments in Japan and India made announcements in 2010 about public sector clouds. Governments are concerned both with the threat of cyber attack and the dangers of intrusion in remote or co-located facilities, both at home and abroad. Strict regulations concerning the privacy and protection of citizens' data directly impacts their data centre operations and the protection measures required in response to legislation.

Levels of protection demanded of their suppliers will vary by individual customer

Many customers have private cages with their own keys or cards and do not allow access to them by third party staff. Wholesale customers may have their own protection in place and use of biometrics for access. Protection may be less specific in shared co-location facilities.

Customers have less control over managed or hosted software services where the physical data centre is not part of the main offering. It is then incumbent on the service provider to ensure their physical IT assets are protected on behalf of their customers. Service level agreements are currently relied as the main means of assuring service quality and availability.

A customer using telco services may want to place restrictions on physical access to their own cabinets/cages - enforcing a 'no touch' type policy for both the managed telco service provider and any other third party wholesale operator being used by a telco.

Telcos themselves maintain large configuration management databases (CMDB) which hold technical details at POPs (point of presence) of all their assets (routers, cabinets, cabling networks, repeater stations). CMDB are the responsibility of facilities management, engineering or the co-location team, depending on the type of data centre model in operation. This CMDB also requires physical protection and auditing.

As corporate information moves out beyond the secure perimeters of company facilities into the wider Internet world, physical protection of assets becomes as vital to the business as combatting the threat of cyber attacks.

2. CURRENT FOCUS ON BUILDING SECURITY AND HUMAN ACCESS TO THE DATA CENTRE DOES NOT ADDRESS NEW DEMANDS OF IT ASSET PROTECTION FOR CLOUD COMPUTING

REGULATORY COMPLIANCE

Regulatory compliance is a key business driver. As more company data is hosted in third party data centres, compliance becomes an important factor in where and how IT assets are located and protected. In cloud services, a distinction is made between the cloud *controller* (who owns the data and bears responsibility for it) and the cloud *processor*. Business users are legally responsible for their data even when it is outsourced or hosted elsewhere.

Business value depends heavily on the smooth running operations of IT and continuous availability of information assets. Shareholder value can be severely damaged by environmental accidents or inadequately managed operations. Theft, damage, overheating, fire, smoke damage or network outage are all on the risk agenda.

Risk management is challenging in today's fast moving technological environment. Not only are cyber threats a concern but network configurations are constantly changing according to business needs. Mergers and acquisition introduce additional complexity in terms of network harmonisation and asset protection. There is usually downward pressure on costs.

A decision to outsource data centre operations or use co-location, managed or cloud computing services, does not mean that business managers abrogate their responsibility to keep company data secure - their legal obligations remain the same. Going forward, companies have to find even better ways of controlling and auditing their information assets.

Legislative drivers behind increasing physical protection

Companies must be able to report on the level of risk being carried by their organisations. This is a matter of legislation in most countries. In the USA, federal laws such as the Gramm-Leach Bliley Act (GLBA); the Health Insurance Portability and Accountability Act (HIPAA) and The Sarbanes-Oxley Act ensure that companies comply with a range of different security and privacy issues.

In the US electric utilities industry, there is also a requirement to secure the power distribution network. Homeland Security Directives dictates that assets that are old and could potentially compromise national security must be secured.

Other regulations may apply at a State level in the United States.

Type	Compliance focus
Sarbanes Oxley (SOX)	Greater auditing of the company's financial system is tied into the IT platform. This leads to more effective auditing with a need to identify and provide a time-based record of when and where the network was accessed and by whom
PCI DSS	A self-regulating, industry consortium standard used by credit card companies to protect consumer records in the database
HIPAA	Used in the US health care industry to protect patient data in hospital computer networks and data centre storage, to ensure that patient privacy is not compromised

US legislation driving the auditing of IT assets
Source: BroadGroup, 2010

Compliance with Sarbanes-Oxley legislation, local country legislation and the Payment Card Industry Data Security Standard (PCI DSS) are the most common areas for compliance amongst US and European companies.

Some non-US governments have enacted legislation which closely follows Sarbanes-Oxley e.g. the Financial Services Authority legislation in the UK. As a result, more than 40 new regulations came into effect in the UK in 2009.

"There is no doubt that the information compliance and governance task is increasing."
Mike Lynch, CEO, Autonomy

In Asia Pacific, the approach varies according to government policies and socio-cultural issues.

In Australia, for example, there is no directly comparable legislation to either the Sarbanes-Oxley Act or the PCI DSS credit card industry regulations. The Australian government does, however, take a strict approach to personal privacy and protection of personal information in the form of its National Privacy Principles. Data processing and data holding in Australia is carried out according to these principles but there is no mandatory reporting of privacy violation - the business decides whether violations should be reported or not. Whilst public information held by a government agency is less likely to be sent to an offshore data centre, commercial organisations are less constrained about shipping trans-border data.

In countries where the individual is of less significance than the state, e.g., Singapore, there is less emphasis on 'private information'.

The Sarbanes-Oxley Act drives corporate governance. Senior executives are personally liable for infringements of data handling and protection laws. US multinationals require business units based outside the United States to demonstrate Sarbanes-Oxley compliance and to be audited annually - even in countries like Australia where this type of legislation is not in force. Many European banks and companies in other sectors have some elements of operation in the USA and many of them apply US regulations to their global operations.

According to an international security expert, one of the outcomes of compliance legislation is that organisations equate governance with finance rather than with behaviour. Many companies do not think through specific business process needs sufficiently before launching new IT projects. Too narrow a view means that companies do not achieve the level of transparency and control that they could if they took a more holistic view of their business.

AUDITING STANDARDS APPLIED TO THE DATA CENTRE

Data centres have often been at the low end of IT and corporate priorities and this is well illustrated by the standards work around data centres. Most of this has focused on other areas of IT and telecoms such as BICSI (cabling), TIA-942 (telecoms) and ASHRAE (cooling). Typically, there is greater investment on the logical security of IT systems and software than on physically protecting data centre assets and infrastructure.

There are a number of data centre standards in use that address primarily the *availability* aspects of data centre security but are weaker on *confidentiality* and *integrity*. These are the three principal properties of information security used by the international standard for implementing an information security management system (ISO/IEC 27001).

International COBIT standards promoted by the ISACA international auditors' organisation are also used in the USA, Europe and Asia Pacific countries.

ISO 27001 Certification is, in essence, business-driven and business-oriented, linking business processes with security needs. Its aim is to drive security from a business and quality perspective, enabling companies to select a number of controls with which to operate a business control framework across all functions of the business - not just IT. In many companies today, this wider purpose is overlooked and IT is typically used as the pilot for, and the driver of, ISO 27001 across the rest of the organisation. ISO 27001 certification is applied widely in the UK and Europe and less so in the Asia Pacific region apart from Japan which accounts for 90 percent of this certification.

ISO/IEC 27001 does not stipulate how risks should be identified and assessed but leaves this for individual organisations to decide.

SAS 70 Type I or Type II Audit Compliance (in use since 1992) is designed to be implemented throughout all areas of the data centre and is used for testing and reporting on the controls in place.

The SAS 70 best practices checklist for data centre physical security addresses:

- Built and constructed for ensuring physical protection
- Protection of physical grounds
- Bullet resistant glass
- Maintenance of vegetation

- Security systems and 24x7 backup power (functioning at all times)
- Cages, cabinets and vaults - properly installed with no loose or moving components
- Man trap - secure access to the data centre floor
- Electronic access control systems (ACS) - only authorised individuals
- Provisioning process - personnel requesting access should be enrolled in a structured and documented provisioning process
- Off-boarding process - closing down specific access by data centre staff or third party personnel once an approved action is completed
- Visitors - properly identified and documented in a ticketing system
- Alarms - hardwired on external doors and sensitive areas
- Cameras - a mix fixed, pan, tilt and zoom cameras in sensitive areas
- Threat conditions policy (consistent with the USA's Department of Homeland Security rating scale)
- Badge and equipment checks
- Local law enforcement agencies
- Paper shredding
- Data centre security staff
- Other activities including response and resolution to security alarms; customer assistance for cage lockouts and escorts.

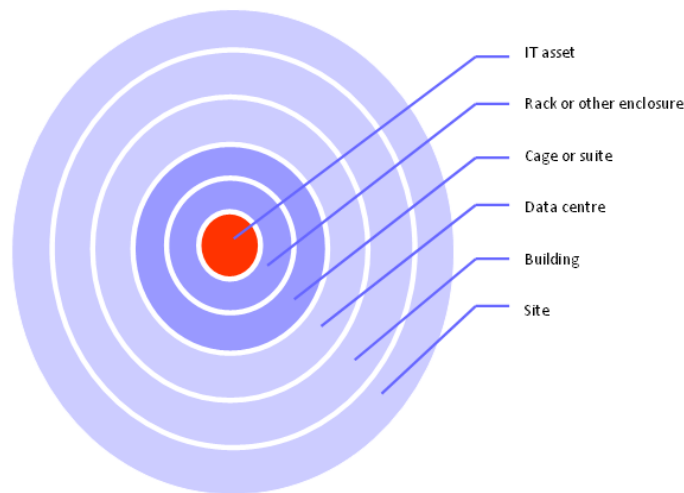
ISO 27001 and SAS 70 Type 2 have become the most important external certifications for data centre providers (primarily in North America and Western Europe) as a means of demonstrating their ability to support customer security efforts. Many third party data centre operators use both ISO 27001 certification and SAS 70 compliance auditing as assurance 'badges' for potential customers evaluating outsourced or hosted data centre service providers.

THE CURRENT APPROACH TO PROTECTION

Layers of protection

Data centre protection includes: site and building security; physical access to the data centre and its contents; human behaviour of employees, vendors, maintenance and other third parties when inside the data centre; environmental monitoring - temperature and humidity levels, power and cooling, hazards to people and infrastructure and emergencies.

The approach to protecting the data centre is multi-layered. The various layers to be protected are illustrated in the graphic below:



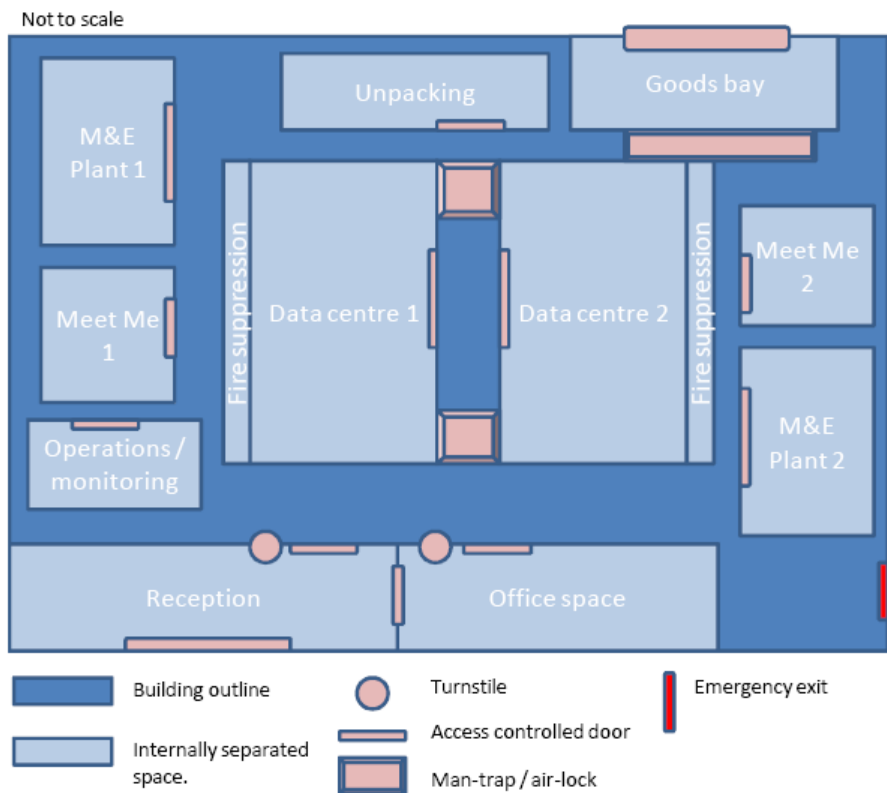
Data centre layers of protection
Source: BroadGroup, 2010

Physical

Physical protection today emphasises building security. Entry controls address a range of human access points around and within the data centre. People (employees, vendors and third party maintenance staff) and goods enter different parts of the data centre via controlled entry points and according to pre-defined company policies and procedures.

A combination of surveillance methods (badges, video, cameras and biometrics) are used to ensure only the right people gain access to server racks but little attention is currently given to auditing a person's behaviour once access has been approved. Human traffic is monitored but not fully tracked and audited in real-time. It has been estimated that more than 50% of the problems in the data centre are caused by accidents or human error.

The next graphic provides a high level view of the physical areas at risk in any data centre:



Data centre layout showing buffering of data centre areas from outer walls
Source: BroadGroup, 2010

Environmental

Environmental hazards include the threat to facilities, equipment and people of fire smoke, and water. Heat and temperature, along with airflows and atmosphere must be carefully monitored and controlled. According to the Network Reliability and Interoperability Council of the US Federal Communications Commission (FCC), 95% of the damage caused in data centre fires is due to smoke and its long-term corrosive effects. Water-related threats stem from many sources both external to the facility (flood or leaking roof) and within it. Internal water threats are more of an issue for data suites or server rooms constructed within existing buildings or in multi-tenanted office buildings (e.g., problems with adjacent tenant's water pipes) than in purpose built data centres.

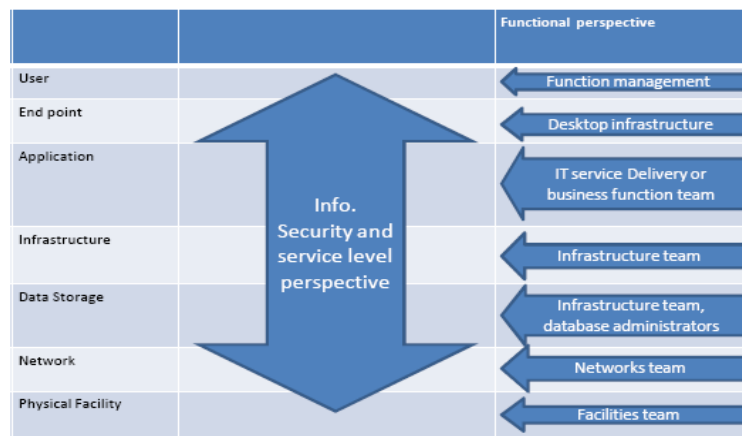
3. CURRENT BEST PRACTICE DATA CENTRE SECURITY, PROTECTION AND CONTROL DOES NOT ENCOMPASS CLOUD COMPUTING AND THE INTERNET OF THINGS

The data centre market is slow moving and is risk averse and takes a long time to change. Lifecycles are typically related to Mechanical & Electrical (M&E) lifecycles of 7 to 10 years rather than to shorter, faster IT lifecycles. In recent years, the data centre sector has focused on design, power and sustainability. The sector is still in the early stages of understanding the implications of cloud computing. It has yet to recognise the operational and customer benefits that could be realised by intelligent asset handling and the use of smart devices.

One of the drivers behind current best practice is siloed responsibilities which prevents holistic thinking.

SILOED RESPONSIBILITIES

In many companies information security and physical security will be managed separately generating weak points and vulnerable security gaps, as well as 'over-securing' and conflicting priorities.



IT Service delivery and security versus functional perspectives

Source: BroadGroup, 2010

Typical management structure in most organisations is not aligned in a way that best serves IT protection, since responsibilities are divided between software development, applications administration, infrastructure administration, network operations and data centre operations. Security may well be the responsibility of a specially designated group or team. Critically, the people who understand the real value of the information or service may sit outside any of these teams.

Current 'narrow' thinking about what IT control encompasses

One explanation for the lack of cohesive thinking about IT is the way senior management views IT within the organisation: "If there is an electron in it, IT must be responsible for it".

Management seems more concerned by the threat of firewall intrusion and cyber attacks than they are about physical security of the IT equipment and infrastructure on which the smooth running of the business so heavily depends. Elements of physical security are cited in Request for Proposals (RFPs) but not always followed through. Too often, physical security stops at the data centre perimeter /front door level. This limited focus on building-only security means that real risks to the business are overlooked. Today, the focus is on detection, delay and response rather than anticipation and tracking for pro-active control, protection and prevention.

The narrow thinking is a barrier to true protection. Physical assets (in or out of the cloud, in transit or 'at rest') are more vulnerable to security breaches than software. According to 'The Microsoft Security Intelligence Report' (SIR)², which evaluates the evolving threat landscape and trends, the largest single category of incidents involved stolen equipment and accounted for 30.6% of the total security breaches in the first six months of 2010. Incidents of negligence (includes lost, stolen and missing equipment or improper disposal) occur more than twice as often as malicious incidents, such as hacking, malware and fraud.

² <http://www.microsoft.com/security/sir/>

4. THE GAPS IN EXISTING SOLUTIONS AND A ROLE FOR THE OF INTERNET OF THINGS

The ‘commoditisation’ of security is changing buyer behaviour. Over the last five years, customers have begun to rely more heavily on vendors for security advice, rather than seeking independent advice from security specialists. As a result, customers are not always selecting products that meet their needs. Furthermore, customers are not always achieving the desired outcomes of larger projects because they are failing to understand the entire end-to-end process implications. Silo thinking and the lack of discussion between business functions reinforces this failing.

CURRENT PROTECTION - VENDOR SOLUTIONS

A wide variety of vendors sell into data centres. Solutions range from full scale building management systems or environmental management systems platforms to point solutions, as illustrated by the examples below:

Type	Focus and trends	Vendor examples
Physical surveillance	Increasingly IP networked cameras /videos Combined with use of biometric recognition Integration with physical rack access	AXIS, Bosch, Pelco, Panasonic, Sony / Milestone, Genentec Fujitsu (biometrics) TZ Inc.
Building management	Integrated provisioning of Building Management Systems, air conditioning & security systems. Major investment.	Honeywell, Johnson Controls, Siemens
Environmental management	Integration with BMS and security - typically early detection and response Environmental sensing solutions for proactive prevention with remote activation	AKCP, APC by Schneider, Honeywell, IBM, Kidde, NEC TZ Inc.
Integrated data halls (modular builds)	‘Ready to go’, pre-assembled containers; can be operated as ‘sealed’ environments Design ideas from other sectors like catering and hospitals are being used (Bladeroom)	HP, Dell, Bladeroom
Micro cabinets	‘Ready to go’ micro-data centre cabinets for use in remote locations - with integral protection	Anixter /TZ Inc.

Type	Focus and trends	Vendor examples
Cabinet/rack protection	<p>Broad range from mechanical, through electronic locks to web-based fastenings with web-based remote control and actuation.</p> <p>Increasing management over IP.</p> <p>Some products will integrate with building access control, video and power management</p>	<p>Web-based actuation: TZ Inc.</p> <p>IP platforms: NetBotz (APC Schneider), Rittal, Cooper B-Line, NTI, Austin-Hughes</p> <p>Mechanical: Southco</p>
Asset Management software tools	Asset management tools work with other vendor security products	HP, BMC, CA, Tideway, TZ Inc.

Data centre security monitoring - types of products and vendors
 BroadGroup 2010

Some asset protection products are designed to work only in conjunction with own brand vendor products, whilst others will integrate with existing vendor solutions. The majority of the solutions on offer today relate closely to the key elements listed in SAS 70.

Despite the many good measures in place today, potential risks persist (see table). Networked, smart devices will pro-actively control and manage these risk areas.

Protection points	Existing counter measures	Potential risks
Building layout	Mix of physical barriers and staff access controls; CCTV monitoring, & alarms	Emergency exit doors and loading bay doors can be weak points of entry
Staff/visitor access	<p>Central access control system to monitor and report access. Pre-registration of visits. Turnstiles, access controlled door; man-trap or airlock door; keypads, proximity cards and photo badges</p> <p>Biometrics (fingerprints, hand geometry, palm or finger vein geometry, facial characteristics, voice signature, iris pattern, retina and vein geometry</p>	<p>Inadequate verification of human credentials. Proximity card forgotten or borrowed</p> <p>Established policies and procedures may be ignored. Tail-gating by unauthorised personnel</p> <p>Biometrics prone to operational difficulties, Intruders discover ways to dupe biometrics</p>

Protection points	Existing counter measures	Potential risks
Cages & suites	Pre-booked access; visitors escorted by member data centre staff; customer-only keys per cage/suite	Inadequate controls to prevent tampering with other equipment (locks on other cages)
Racks & enclosures	Lockable doors using physical keys or electronic keys - with varying levels of audit trail. Not all electronic locks can be retro-fitted	Server racks with identical locks Key management is cumbersome - keys lost. Locks are often omitted for equipment in private cage or suite or to secure other infrastructure (ports, plugs, cables)
Micro data centres	Many remote locations go unsecured	High level of risk if not remotely monitored and physical access logged and audited
Cabling security	Security standards, e.g., ANSI, TIA & EIA-942	Changes made and not audited; cables or plugs unplugged in error
Environmental	Environmental monitoring systems to control ambient temperature, air flow, humidity levels. Sensors to detect fire and smoke, dust particles and water hazards	Alerts occur too late for preventative measures before component failure occurs. Interrupted continuity of supplies electrical power, communication links, HVAC systems. Staff put at risk
Transport	Assets for disposal	Assets tampered with or removed in transit.

Physical asset protection points in today's data centre and associated risks
 Source: BroadGroup 2010

In the cloud computing and hybrid cloud environments, IT assets are increasingly dispersed throughout the world. Whilst large companies will try and select their data centre locations carefully, it is sometimes unavoidable to locate vital corporate assets in hostile environments (isolated regions, adverse climate conditions, poor maintenance skills) where they are vulnerable to accidental damage, sabotage and theft.

Data centre provision is generally of high quality in world capitals but in some areas of Latin America, Africa and Asia the use of intelligent remote control and actuation of IT assets in remote locations will be of keen interest to governments and multinational organisations.

In hybrid, hosted and managed service environments, the deployment of smart devices in the service provider's data centre could become an essential component for customers in future service level agreements. Cloud introduces multi-party contractual regimes (e.g., Software-as-a-Service is provided on other platforms in collaboration with partners such as Amazon). Users will want to know that all the providers in their supply chain have proper physical asset protection.

As cloud services develop, vendors are also looking at the changing contractual requirements. Microsoft, e.g, is currently funding a three year project at Queen Mary, University of London, looking at legal issues and terms of service in the cloud.

THE INTERNET OF THINGS IS THE FUTURE PLATFORM FOR PROTECTING IT ASSETS

The Internet of Things will protect customer assets in the cloud or at a remote locations - and help data centre operators meet the demanding requirements associated with cloud service delivery.

In terms of protecting IT Assets 'out there', the Internet of Things supports:

- Granular access control
- Stand alone security
- Detailed and real time audit trails
- Risk management
- Remote control
- Compliance with regulation

In terms of helping hosted service providers to meet the new demands of running of data centres in the cloud, the Internet of Things supports:

- Smart sensing and metering
- Remote control
- Compliance with regulation

The ability to connect small, inexpensive devices directly to the Internet has only recently been realised but the advantages of this are numerous and powerful - not least in the data centre. Operations will become increasingly dependent on The Internet of Things as cloud services evolve. Use of intelligent devices and micro-protection will be essential to manage the scope and complexity of service provision.

Cloud computing is evolving fast and a variety of clouds are on the horizon. These include specialist sector clouds (health, pharmaceutical, financial trading); community clouds (hybrid of private and public cloud in education or local government); national clouds addressing local laws and data protection. Federated cloud services which will work seamlessly together in a standardised way are anticipated. These highly automated environments will depend on intelligent asset handling for their smooth running.

5. EMERGING TRENDS IN THE 21st CENTURY

Modern asset protection requires holistic thinking. ‘Prevention is better than cure’. Operational benefits and cost savings can be achieved by linking related (and sometimes seemingly unrelated) processes and events. Advances in technology and web-based platforms enable companies to look at old problems in new ways - and this includes physical asset protection. The Internet of Things means new ways of offering both local and remote protection (from human, environmental hazards and threats), as well as remote control and visibility. Next generation technologies, now emerging on the market, offer innovative approaches to protection. An interesting example of this is TZ Inc.’s smart micro-protection systems (ixp.tz.net) which use shape memory alloy actuated intelligent locking devices for advanced protection and remote control of assets. This unique approach to electro-mechanical locking appears to enable a range of devices with much smaller form factors and less power consumption.

TZ Inc.’s web-based platform provides real-time audit trails and remote actuation. Their intelligent locking devices work with existing structured cable (or wireless networking) and will open - and close – on command according to customer’s specification. Cabinet doors, shelves, servers, tiles and plugs can be checked remotely. Devices are locked and unlocked remotely via a user portal. This technology is fully IP addressable and fully auditable. The TZ Inc. platform is also being used to ensure last mile chain of custody of accountable mail and parcel delivery through an intelligent storage system using a network of their locking devices.

Technologies like these will open up new horizons in asset and infrastructure protection - both in the data centre and in other parts of the customer’s business operations (retail outlets, hospital and research labs, government departments).



The 21st century asset protection approach
Source: BroadGroup, 2010

A major advantage of these emerging smart device systems like TZ Inc’s technology is their ‘universal application’ and multi-purpose qualities. In the data centre environment, for example, it will protect and control both physical access and environmental (e.g. cabinet over-heating) conditions. It can provide monitoring control both *inside* and outside a rack or cabinet. It can be deployed by very large organisations in mega data centres as well as users with single cabinets.

Another advantage is that, via the Web portal, customers have full visibility and remote control of their physical assets - even when they are outsourced to a third party or hosted managed service provider - and are aware of alarms in real-time. This places control firmly back in the customer hands. It introduces new aspects to the supplier /customer relationship.

Interviews with a range of customers that are currently using smart device micro-protection systems (specifically TZ Inc.'s Praetorian or Centurion infrastructure protection systems) provided the following feedback:

US Organisations	User experience
Co-location and cloud hosting service provider	Client mix of large companies, SMEs and start-ups in various sectors Network infrastructure is constantly changing Audit information is used for the data centre's own compliance and management <i>"The system is very secure and very user-friendly and not intrusive. People like convenience. They don't like inconvenience or the bother of finding keys."</i>
University campus	Two data centres - one large, being expanded. Both with 24x7 access. Used in conjunction with camera technology. <i>"A key factor in buying was the control element of tracking human behaviour"</i> <i>"We can pinpoint exactly who was there and when - and prove it."</i> <i>"It is an extra layer of security - vendors now have to specifically request front or back of cabinet that is to be opened remotely."</i> <i>"We have a report at our fingertips if we need it."</i>
State tax board	Campus environment with two very large data centres and 4,500 employees Consolidation has introduced co-location with other government agencies Critical need to comply with Federal laws to protect citizen data and provide 2 physical barriers between personal data and access to it - beyond badge access and cameras. <i>"The challenge we face is how to open up the data centre but keep access secure."</i>
IT systems & software vendor	Production data centre acts as internal co-location facility for the group's diverse businesses - all concerned about protecting their own data in a shared environment <i>"The locking system allows us to set time windows for certain repairs."</i> <i>"It tracks when work occurs and prevents accidental entry into a cabinet - which happens when people are not paying attention and can just open up."</i> <i>"The system is cost-effective -it does not need a separate card lock on every door."</i>

User experience of smart device micro-protection systems
 Source: BroadGroup, 2010

Other benefits that this next generation technology brings to data centre customers are:

- **Easy to deploy and integrate** - can be retrofitted to existing plant and overcomes the magnetic field problems associated with traditional security locks on metal doors.
- **Helps control costs** - 'one lock fits all' philosophy and '2 locks (back and front)' bypasses 'specific locks for a specified rack' and high numbers of locks per rack.
- **Combines physical and environmental protection** effectively in one system.

"The TZ system is more complete and very simple to install -and control is moving to the end user"
European systems integrator

INTEGRATING ASSET PROTECTION WITH BUSINESS PROCESSES

The rapid growth of IP platforms and cloud computing services is changing the way companies operate and manage their business. The alignment of IT with business objectives puts new demands on information management. In turn, the convergence of IT and security means that traditional approaches to security within the data centre are becoming outdated and unfit for purpose. Sophisticated technologies like micro-protection means that service providers and customers in private and public sectors can take a more comprehensive approach to asset management and risk management. In the 'Internet of Things' environment, companies can track with ease, and have real-time proof of 'what goes on where and by whom' or thing.

Importantly, information harvested from tracking physical assets in real time, will provide business managers with valuable information that can be used for compliance, problem resolution, HR and customer service.

The key business process areas which micro-protection of physical assets will support include:

- **Corporate governance**

The database will automatically generate the management reports required to meet sector and company compliance obligations. Data can be directly uploaded by Finance Directors (e.g. for Sarbanes Oxley), Human Resources (e.g., for HIPAA) and Business and IT Directors (e.g., for SAS 70 or ISO 27001).

- **Workforce management**

Micro-protection auditing can be linked to 'request and approval' processes for vendors and third party maintenance suppliers. IT can be used (depending on national and corporate policies in place) to identify segregation of duties, reporting actions taken by building, IT and security officers. It can be used for planning workflows and maintenance schedules in IT and data centre facilities.

- **Workforce analytics**

Audit trails can be used by Human Resources or team managers for monitoring employee productivity and time management across business functions and sectors.

- **Health and safety compliance**

Human traffic in hazardous environments can be monitored and access prevented if dangerous environmental conditions arise, e.g., restricting access to certain areas if temperatures rise to unacceptable levels; or taking pre-emptive action by opening up equipment or locking it down according to pre-set business rules.

- **Property management**

Auditing and reporting of security systems deployed on real estate (e.g., cameras and video surveillance, biometric systems) for inventory management and maintenance.

- **Network design and build infrastructure**

Moves and changes of critical computing and cabling infrastructure can be monitored in real-time, automatically generating management records for future reference.

- **Network operations and maintenance**

Micro-protection improves information around operation and access of personnel in the data centre and inspection (generating visit reports for clients). Visits can be traced in detail. Access controlled to the micro level in real-time.

Advanced M2M solutions enable corrective and emergency maintenance of fixed assets, 'remote hands' control and time-based predictive maintenance. Plant and equipment, cabinet doors and temperature can be checked in a virtual environment. Cabinet doors can be automatically shut down in environmental emergencies or in the event power failure to prevent manual operation if company policies so require. Remote actuation means that locks on assets can be programmed to release according to specific pre-set environmental conditions or instructions. Assets and devices that are micro-protected can be geo-tagged, tracked and protected at rest or in transit (using RFID wireless technology) when moved for storage or disposal at another site or location. Geo-tagging can be applied to warehousing, logistics and inventory management of all types of devices.

Remote local or global facilities (in-house or third party) can be inspected, via the Web portal, according to customer policy and business needs. This is a powerful advantage for enterprise customers, giving them an element of control previously unknown.

- **Billing and invoicing**

Detailed real-time records of timed access to assets by maintenance engineers can be used to verify work done at the micro-level and used for customer billing. Micro-metering and billing of power consumption would be another application.

- **Customer service**

Remote monitoring and reporting on the real-time status of customer assets in a third party location allows customers to maintain a crucial element of control. Remote actuation by the customer himself (not the service provider) gives the customer total control over his assets. Potential disputes can be avoided.

- **Developing new services**

Service providers will be able to generate monthly customer service level reports by using collected data on sensor and locking mechanisms. These will give customers factual information on the state of their assets against service level agreements.

Smart service providers recognise that advanced micro-protection, monitoring and remote control provides them with opportunities for delivering innovative, value added services to customers that satisfies the need for higher levels of control in an increasingly virtual environment.

CONCLUSION

The Internet of Things brings new ways of giving control back to users and to suppliers of cloud computing services. This next generation of networked smart devices provides a sound foundation for protecting physical assets as cloud computing advances to the next level. It provides an added dimension of assurance for both users and providers of hosted services.

Growing convergence of IT and security means that organizations must take a more holistic view of 'security' in general. Micro-protection will become a critical element of risk management strategies going forward. The ability to integrate physical asset protection with other business processes elevates cross-functional working to a new level. It will enhance both compliance and business performance.

The combined force of cloud computing and the Internet of Things signals a new phase in operational best practice, where IT and the business are more seamlessly aligned and where technology serves the business.

About BroadGroup

BroadGroup is the leading consulting firm in the data centre sector and undertakes a specific set of consultancy services including international market entry, competitor analysis, marketing audits and commercial due diligence.

BroadGroup Consulting
Stonebridge House
28-32 Bridge Street
Leatherhead
Surrey
KT22 8BZ
United Kingdom
T +44 (0)1372 869620
F +44 (0)870 9223452
www.broad-group.com
www.datacentres.com

Every effort has been taken to ensure the accuracy and completeness of information presented in this report. However, BroadGroup cannot accept liability for the consequences of action taken based on the information provided.