White Paper
Data Centre Vulnerability

In recent months more emphasis has been given to the security of data, considering the rapid expansion of the Internet of Things (IoT). This in turn has raised the subject of the vulnerability of the facility that is holding or storing that data.

There have been two studies published in the last 18 months that back this up. The first, related to PoE-enabled devices, forecasts the market growing by over 19% and achieving sales in excess of $1 Billion in 2021. The second survey estimated that there will be 36 Billion IoT connected devices by 2021, reaching 75.5 Billion by 2025. With this rate of growth, the security surrounding the storage of the data is critical.

Whilst there is a lot published regarding the importance of cyber security, quite rightly, there has been very little coverage regarding the other vulnerabilities surrounding Data Centres. There are two key areas we must consider that could affect the ongoing performance of the DC.

Housekeeping

The first relates to what I call 'Housekeeping'.

Good Housekeeping is essential and that can also be split into two parts, the first relating to the containment. Whilst the initial design may have been 'fit for purpose' when it was first constructed it can soon become overwhelmed if complacency creeps in. Too often I see cables left in situ because records of connectivity are not being maintained correctly. This then leads on to the 'Fear Factor'. If a member of staff doesn't know what cable is connected to or it is too difficult to remove, it gets left and they take a new patch lead out of the bag and install it. This soon gets out of hand and the containment overflows with redundant cables.

This leads to one of two things happening, examples for both of which I can draw from personal experience. For the first scenario (I cannot mention names, all I can say it was a DC operated by one of the major high-street supermarkets) I was called to site to review part of the existing cabling installation and make some recommendations regarding expanding the data hall as they wanted to add more cabinets. When I first entered the room, I was struck by noise of the CRAC units on the walls - they were working at almost maximum capacity. The room wasn't overly hot however the problem was the design. In this DC, all the cables – both power and data – were run underneath the raised floor. This space was also an air handling space with the cold air supply. No cables were routed at high level. When raising some of the tiles the culprit was obvious; they had undergone a number of upgrades to equipment over the years, but they had never removed any of the old redundant cable as they didn't have good enough record keeping to understand which cables were unused and which were critical to DC performance.

Whilst this DC did not ultimately fail, it did result in a very expensive transition plan, which involved the lease of an external data hall whilst this one was completely redesigned and rebuilt. It was a very long and expensive process that took more than a year to complete. It must be noted that the original DC had been first designed and built in the mid-1990s when computer equipment and connectivity was totally different and they just kept trying to fit more equipment in.

The second example is related to a finance organisation, where they had to document and replicate a complete redundant cabling and patching field within one of their data halls before transitioning one of their existing cabling systems over to the third one with overnight working, then rectifying, correctly labelling and documenting the offending system before putting it back in service and then removing the original redundant system. This work took over 3 months to complete and cost in excess of £250,000.

The second element regarding good housekeeping comes down to cleanliness. With all DC environments it is essential that the greatest level of cleanliness is maintained. I see too many DCs, especially those used by smaller organisations, where poor practice is rife. Unfortunately, there are two different groups that work in the data hall; you have 'IT people' and 'cabling people' operating in tandem and never the twain shall understand each other's problem.

Too many times I see a data hall or main comms room being used as yet another storage cupboard for old equipment and packaging. With all of this comes dust, one of the biggest enemies to efficient operation of a fibre infrastructure. Fluke research states that 85% of all fibre faults derives from end-face contamination. NTT state that in excess of 80%, therefore this is the number ONE problem with fibre connectivity.

Best practice dictates that all packaging should be removed outside and never taken into the data hall itself.

Physical Security

It is not just the threat of cyber-attacks that we need to be concerned about, it's also the physical security of the infrastructure that is under threat. Standards bodies have not been slow in reacting. Cenelec published EN 50600-2-5 in 2016, Information Technology – Data Centre facilities and infrastructures – Security Systems. The ISO/IEC 22237-6, based on the content of the Cenelec standard, was published in 2018.

In parallel to this activity in 2016, the ANSI/TIA- 5017 - Telecommunications Physical Network Security Standard was published. This doesn't just look at Data Centres, it covers the whole physical infrastructure.

There are several key differences between the Cenelec/ISO and ANSI/TIA standards. Therefore in 2018 ISO/IEC JTC1/SC25/WG3 agreed to come up with an international version of the latter. The committee draft of ISO/IEC CD 24383 was published in 2019 and is now out for final comment.

ANSI/TIA-5017 describes three Security Levels as follows:

- **SL1 - Basic Security Installation:** Installations that follow the guidelines in the TIA TR-42 family of cabling infrastructure standards with minimal additional security and protection levels. This is typically used in all installations where there is a desire to build a secure network infrastructure and protect security cabling and network traffic from unauthorized access or interruption.
- **SL2 - Tamper Resistant Installation:** Installations that reduce the possibility of tampering or damage to the premise where there is added risk, vulnerability and the need for higher security to protect the infrastructure and the network traffic.
- **SL3 - Critical Security Installation:** Installations intended to achieve a security level where the level of risk is considered high and the best protection practices are required. This typically covers installations where the security of the network infrastructure and information is critical.

While ISO/IEC TS 22237-6 (for data centres) specifies four Protection Classes as shown below but that all telecommunications infrastructure shall be in spaces complying with its requirements for Protection Class 3 (with monitoring requirements for pathways that are not in Class 3 spaces).

	Protection Class 1	Protection Class 2	Protection Class 3	Protection Class 4
Protection against unauthorised access	Public or semi-public area	Area that is accessible to all autorised personnel (employees and visitors)	Area restricted to specified employees and visitors (other personnel with access to Class 2 shall be accompanied by personnel autorised to access Class 3 areas).	Area restricted to specified employees who have an identified need to have access (other personnel with access to Class 2 or 3 areas shall be accompanied by personnel authorised to access Class 4 areas).
Protection against internal fire	No special protection applied	The area requires to be protected against fire by a detection and suppression system which maintains the function of that area during a fire in that area or one in a Class 1 area	The area requires to be protected against fire by a detection and suppression system which maintains the function of that area during a fire in that area or one in a Class 1 or Class 2 area.	The area requires to be protected against fire by a detection and suppression system which enables critical data centre function to be secured during a fire in that area or one elsewhere in the data centre.
Protection against other internal environmental events	No special protection applied		Mitigation applied	
Protection against unauthorised access	No special protection applied		Mitigation applied	

This demonstrates a subtle difference in approach since the ISO/IEC TS 22237-6 describes who can access spaces (before defining the security solutions of such spaces) and what protection against fire is applied, whereas ANSI/TIA-5017 describes the solutions of the installation of the telecommunication infrastructure in any space.

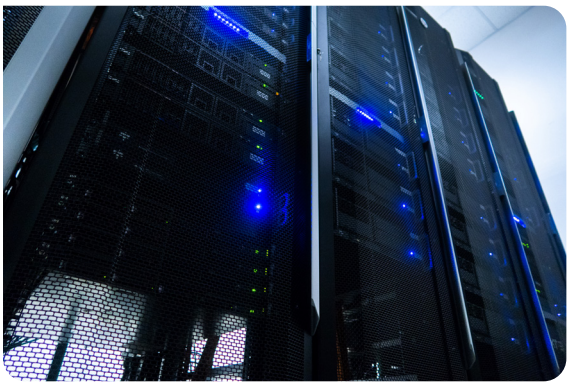
Proposal for development of ISO/IEC CD 24383

With regards to the SL system in ANSI/TIA-5017, the differentiation of the Levels involves vague wording such as “high”, “higher”, “added” in relation to risk and “best” in relation to practices. These are all words that Cenelec and ISO/IEC try to avoid.

The alternative is to consider the solutions first as shown in the following table:

Topic		Security Grade 1	Security Grade 2	Security Grade 3
Pathways	Access control	x	✓	✓
	Intrusion resistance	x	✓	✓
	Monitoring	x	x	✓
Spaces	Access control	x	✓	✓
	Intrusion resistance	x	x	✓
	Monitoring	x	x	✓

So to sum up, ANSI/TIA-5017 has three Security Levels in relation to practices. ISO/IEC TS 22237-6 on the other hand has four protection classes with more detail. Hence an alternative approach which (a) brings the two standards closer together and (b) avoids vague statements of risk and solutions, has been taken to adopt three Security Classes with more clarity in ISO/IEC CD 24383.



Continued collaboration is being given more emphasis to maintain and update the standard as 5G. IoT continue to accelerate their deployments. With all the hard work that has gone into developing standards it is important that not just DC operators are aware of them, but all infrastructure managers.

European Headquarters
Excel House
Junction Six Industrial Park
Electric Avenue
Birmingham B6 7JJ
England

T: +44 (0) 121 326 7557
E: sales@excel-networking.com

Mayflex MEA DMCC
Office 22A/B
AU (Gold) Tower
Cluster I
Jumeirah Lake Towers (JLT)
Dubai
United Arab Emirates
PO Box 293695

T: +971 4 421 4352
E: mesales@mayflex.com

www.excel-networking.com