TECHNOLOGY GROUP

WHITE PAPER

# Beyond Firewalls: Why Electromagnetic Security is Becoming a Critical Requirement for Modern Data Centres

## Electromagnetic security (EMSEC), RF shielding and infrastructure hardening for secure data centre environments.


Author

David West

Head of Secure Shielded Solutions, APC Technology Group


Data centres sit at the heart of today's digital economy, yet one area of their security remains frequently overlooked, the physical and electromagnetic security of the infrastructure itself.

Sophisticated adversaries may target the electromagnetic emissions generated by IT equipment and communications infrastructure. This paper examines electromagnetic security, RF shielding and infrastructure hardening as components of a comprehensive cyber resilience strategy.

Contents

Section 01

# Introduction

Data centres sit at the heart of today's digital economy, supporting cloud services, financial transactions, healthcare systems, defence operations and critical national infrastructure. Furthermore with the rapid growth of AI and high-performance computing (HPC) facilities is driving unprecedented rack power densities and electrical complexity within modern data centres.

As power consumption, switching speeds and infrastructure density increase, electromagnetic compatibility (EMC) and electromagnetic resilience become increasingly important considerations alongside traditional cyber security controls. As cyber threats continue to evolve, organisations are investing heavily in network security, endpoint protection and threat detection technologies.

In the UK, this broader approach to protecting critical infrastructure is reflected in guidance from the National Protective Security Authority (NPSA) and the National Cyber Security Centre (NCSC). Together, they advocate a defence-in-depth approach that integrates cyber security, physical security, personnel security and technical security to improve organisational resilience.

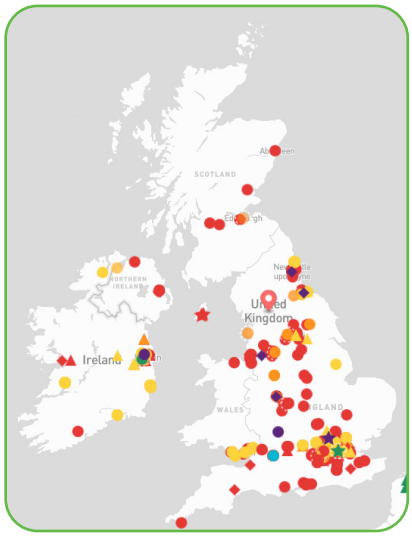


**Figure 1:** Map of data centres in the UK. Baxtel.com

While neither organisation mandates RF shielding for commercial data centres, both encourage organisations to adopt proportionate, risk-based protective measures that reflect the sensitivity of the information and services being protected. However, one area remains frequently overlooked, the physical and electromagnetic security of the infrastructure itself. The importance of this infrastructure is now formally recognised.

Data centres were designated critical national infrastructure in September 2024, the UK hosts more of them than any other country in Western Europe and the sector generates an estimated £4.6 billion in revenue each year.[1]

While traditional cyber security focuses on protecting data in transit and at rest, sophisticated adversaries may target the electromagnetic emissions generated by IT equipment, communications infrastructure and critical systems. These risks are particularly relevant to organisations handling classified, regulated, commercially sensitive or mission-critical information. As a result, electromagnetic security (EMSEC), RF shielding and infrastructure hardening are becoming increasingly important components of a comprehensive cyber resilience strategy.

## The Missing Layer in Data Centre Security

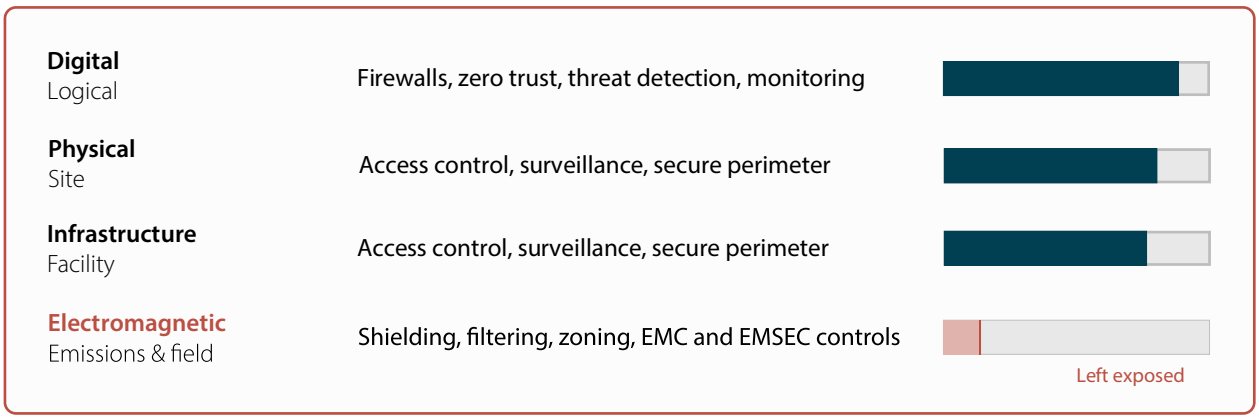


**Figure 2:** Where security investment concentrates across the data centre stack. The electromagnetic layer sits below the coverage line.

### The expanding threat landscape

The modern data centre must contend with a growing range of threats, including the following.

- Ransomware attacks
- Nation-state cyber operations
- Advanced Persistent Threats (APTs)
- Insider threats
- Supply chain compromise
- Physical intrusion
- Communications interception
- Electromagnetic eavesdropping
- Electromagnetic interference (EMI)
- Critical infrastructure disruption

While software-based security controls are essential, they cannot mitigate every attack vector. Organisations must also consider how information can be exposed through the physical operation of electronic systems.

Section 02

## Understanding electromagnetic security (EMSEC)

Electromagnetic security (EMSEC) refers to the protection of information-bearing signals from compromise through unintended electromagnetic emissions.

Electronic devices generate electromagnetic radiation during normal operation. Under certain conditions, these emissions may be captured, analysed and exploited to reconstruct sensitive information. This is not a new or theoretical concern.

The first unclassified analysis of the risk was published in 1985, and research at the University of Cambridge has since shown that modern flat-panel displays are at least as vulnerable as the equipment of that era, because the high-speed digital signals that drive them leak emissions a nearby receiver can recover. [5,6]

This phenomenon is often referred to as compromising emanations, signal leakage, electromagnetic eavesdropping or side-channel interception.

For organisations operating in high-security environments, protecting against these threats is a recognised security requirement. Examples include the following.

- Government agencies
- Defence organisations
- Intelligence services
- Financial institutions
- Critical national infrastructure operators
- Research facilities
- Data centres hosting highly sensitive workloads

Section 03

## Regulatory and standards requirements

As cyber security regulations mature, organisations are increasingly expected to demonstrate robust physical and environmental protections alongside traditional IT controls.

The frameworks below all point towards the same objective, resilient environments capable of protecting critical information and infrastructure.

### The expanding threat landscape

The modern data centre must contend with a growing range of threats, including the following.

| Standard | What it addresses | Gap it leaves for shielding |
|---|---|---|
| ISO 27001 | Physical and environmental security controls within information security management[3] | Risk assessment determines need |
| NIS2 Directive | Risk management and incident reporting duties for in-scope operators[4] | No specific mention of RF shielding |
| NPSA Protective Security Guidance | Physical security, technical security, secure facility design and risk management[2] | Risk-based guidance rather than prescriptive requirements |
| NCSC guidance | Cyber resilience and defence in depth, facility design[8] | No EMSEC performance criteria |

### TEMPEST and secure facility requirements

For organisations handling highly sensitive or classified information, electromagnetic security is governed by specialised standards and frameworks. TEMPEST is a term commonly used to describe the study and control of compromising emanations from electronic equipment.

The objective is straightforward, to prevent sensitive information from being reconstructed from unintended electromagnetic emissions. Although often associated with military and intelligence environments, the underlying principles are increasingly relevant to critical infrastructure and high-security commercial environments.

While these attacks require specialised expertise and equipment, physical access to target systems is not always necessary. Under certain conditions, unintended electromagnetic emissions may be intercepted and analysed remotely, making emission security an important consideration in high-assurance environments.

For defence-related environments, NATO SDIP-27 provides standards for the protection of classified information against compromising emanations.[8]

The framework establishes requirements for shielded environments, equipment separation distances, electromagnetic zoning, facility design and risk-based protection measures. Although not every data centre requires NATO-level protection, the concepts provide valuable guidance for organisations managing highly sensitive information.

Section 04

## Why electromagnetic interference (EMI) matters

Data centres increasingly operate at high power densities, with large concentrations of servers, networking equipment and communications systems. Without effective electromagnetic management, operators may experience signal degradation, equipment malfunction, communications disruption, reduced reliability and regulatory compliance issues.

As AI and high-performance computing workloads continue to increase, electromagnetic compatibility (EMC) considerations are becoming more important than ever. A secure data centre must not only prevent data leakage but also maintain a stable electromagnetic operating environment.

Section 05

## RF shielding as a technical security control

RF shielding is often viewed as an engineering solution, but it also serves an important cyber security function. Shielded environments restrict the transmission of electromagnetic signals into and out of protected areas.

### Applications:

- Secure data halls
- Security Operations Centres (SOCs)
- Defence facilities
- Intelligence environments
- Critical infrastructure control rooms
- Secure communications facilities

### Benefits

- **Protection against electromagnetic eavesdropping**
  RF shielding reduces the risk of information leakage through compromising emanations.
- **Reduced attack surface**
  Shielded environments help prevent unauthorised interception or monitoring of sensitive systems.
- **Enhanced infrastructure resilience**
  Protection against external electromagnetic disturbances improves operational reliability.
- **Support for high-assurance security requirements**
  Shielding can form part of a wider security architecture supporting EMSEC and TEMPEST-related objectives.

Section 06

## The critical role of RF filters

Even the most effective shielded room can be compromised if power and communication services create pathways for unwanted signals. RF filters are designed to protect these entry and exit points. Typical applications include incoming power supplies, data connections, telecommunications links, building management systems and operational technology networks.

RF filters help to preserve shielding effectiveness, prevent conducted emissions, reduce electromagnetic interference and support secure facility operation. Together, RF shielding and RF filtering provide a comprehensive approach to electromagnetic protection.


**Figure 3:** A shielded room is only as effective as its weakest penetration. Power and communication services must pass through RF filters rather than create pathways for unwanted signals.

Section 07

## Building defence-in-depth for modern data centres

The most resilient data centres adopt a layered security strategy. By integrating these layers, organisations can significantly reduce exposure to both conventional cyber threats and more sophisticated forms of information compromise.

| Layer | Controls |
|---|---|
| **Digital security** | Firewalls, zero trust architectures, threat detection and security monitoring |
| **Physical security** | Access control, surveillance systems, secure perimeters and visitor management |
| **Infrastructure security** | Power protection, environmental monitoring, redundant systems and business continuity planning |
| **Electromagnetic security** | RF shielding, RF filtering, EMC compliance, EMSEC controls and NPSA-aligned protective security measures |

Section 08

## How APC Technology Group supports secure data centre environments

As cyber security requirements continue to evolve, organisations are increasingly recognising that information protection must extend beyond software and network controls. APC Technology Group supports customers in developing secure, resilient infrastructure through specialist electromagnetic protection technologies, including:

- RF shielding systems
- Shielded rooms and enclosures
- RF filtering solutions
- EMC mitigation solutions
- Infrastructure hardening measures
- Secure facility consultancy and implementation support

**Design the electromagnetic layer in with APC**

APC Technology Group is a leading distributor across the UK & IE for rf shielding solutions from filters, enclosures and shielding to turnkey accredited facilities.

Start a conversation with one of our technical engineers today

Section 09

## Conclusion

The cyber protection requirements of modern data centres are changing. While network security remains fundamental, organisations must also address the physical and electromagnetic risks associated with increasingly sophisticated threat actors.

Frameworks such as ISO 27001, NIS2, NSPA, NCSC guidance and defence-sector standards all point towards a common objective, creating resilient environments capable of protecting critical information and infrastructure. For organisations operating in high-security environments, RF shielding, RF filtering and electromagnetic security controls are becoming important elements of a comprehensive cyber resilience strategy.

As data becomes more valuable and threat actors become more capable, protecting information at every layer of the infrastructure stack is no longer a specialist consideration. It is a business-critical requirement.

About the author

David West is Head of Secure Shielded Solutions at APC Technology Group, where he leads the company's strategy for secure shielded environments supporting defence, government, critical infrastructure, and high-security commercial applications.

With extensive experience working alongside defence primes, systems integrators, and specialist contractors, David has helped organisations deliver secure electromagnetic environments that meet the demanding requirements of modern classified programmes.

Throughout his career, David has specialised in secure shielding, EMC, and test and measurement technologies, combining technical expertise with a strong understanding of the operational and commercial challenges facing the sector. He works closely with customers to develop practical, compliant solutions that protect sensitive information and enable mission-critical capability across defence and increasingly within data centre environments.

---

## References


1. Department for Science, Innovation and Technology. Data centres to be given massive boost and protections from cyber criminals and IT blackouts. Press release, 12 September 2024.
2. National Protective Security Authority, NPSA Data Centre Security - Guidance for Owners. 8 March 2022.
3. ISO and IEC. ISO/IEC 27001, information security management systems.
4. European Union. Directive (EU) 2022/2555 (NIS2), measures for a high common level of cybersecurity across the Union.
5. van Eck, W. Electromagnetic radiation from video display units, an eavesdropping risk. Computers and Security, volume 4, 1985.
6. Kuhn, M.G., University of Cambridge. Electromagnetic eavesdropping risks of flat-panel displays. Privacy Enhancing Technologies workshop, 2004.
7. NATO. SDIP-27, protection of classified information against compromising emanations.
8. National Cyber Security Centre (NCSC). Cloud security guidance. Principle 2: Asset protection and resilience, 7 June 2023.


## Figures

1. Figure 1: Map of data centres in the UK. Baxtel.com
2. Figure 2: Where security investment concentrates across the data centre stack. The electromagnetic layer sits below the coverage line. APC Technology Group.
3. Figure 3: A shielded room is only as effective as its weakest penetration. Power and communication services must pass through RF filters rather than create pathways for unwanted signals. APC Technology Group.