GLOBAL

#7

GUNNEBO

Security Matters

Checklist

IS YOUR RECEPTION SECURITY FULL OF HOLES?

+ QUICK GUIDE

EMP protection for servers and IT systems

+ RETAIL SECURITY

How to tackle internal theft effectively

+ ANSSI CERTIFICATION

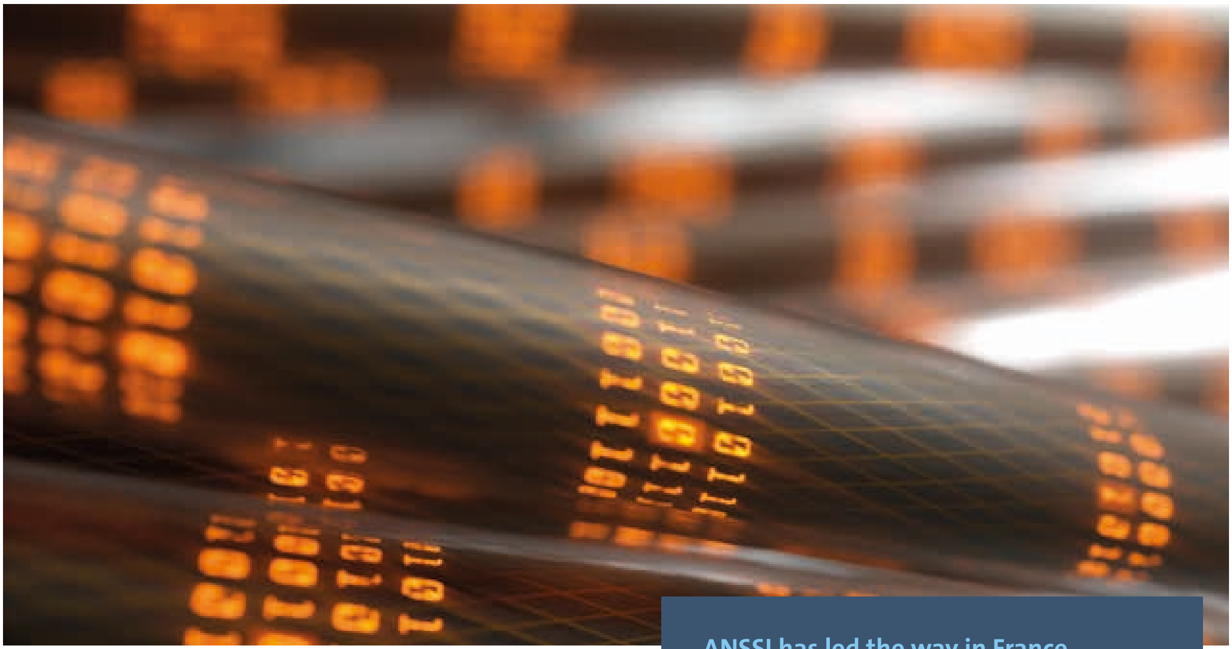
What this means for access control systems

SECURITY MADE EASY

www.gunnebo.com

GUNNEBO®

CONTENTS



ANSSI has led the way in France for establishing regulations for the protection of information.

This edition of *Global Security Matters* looks at what these guidelines mean for security managers in the rest of the world as well as the recommendations it makes for security architectures.

SECURITY MATTERS BLOG

Subscribe for the latest security insights at blog.gunnebo.com.

Quick Guide

EMP Protection for Servers and Vital Electronics

Electromagnetic pulse (EMP) radiation can have devastating consequences for IT systems. But a specially certified server safe can protect against this threat.

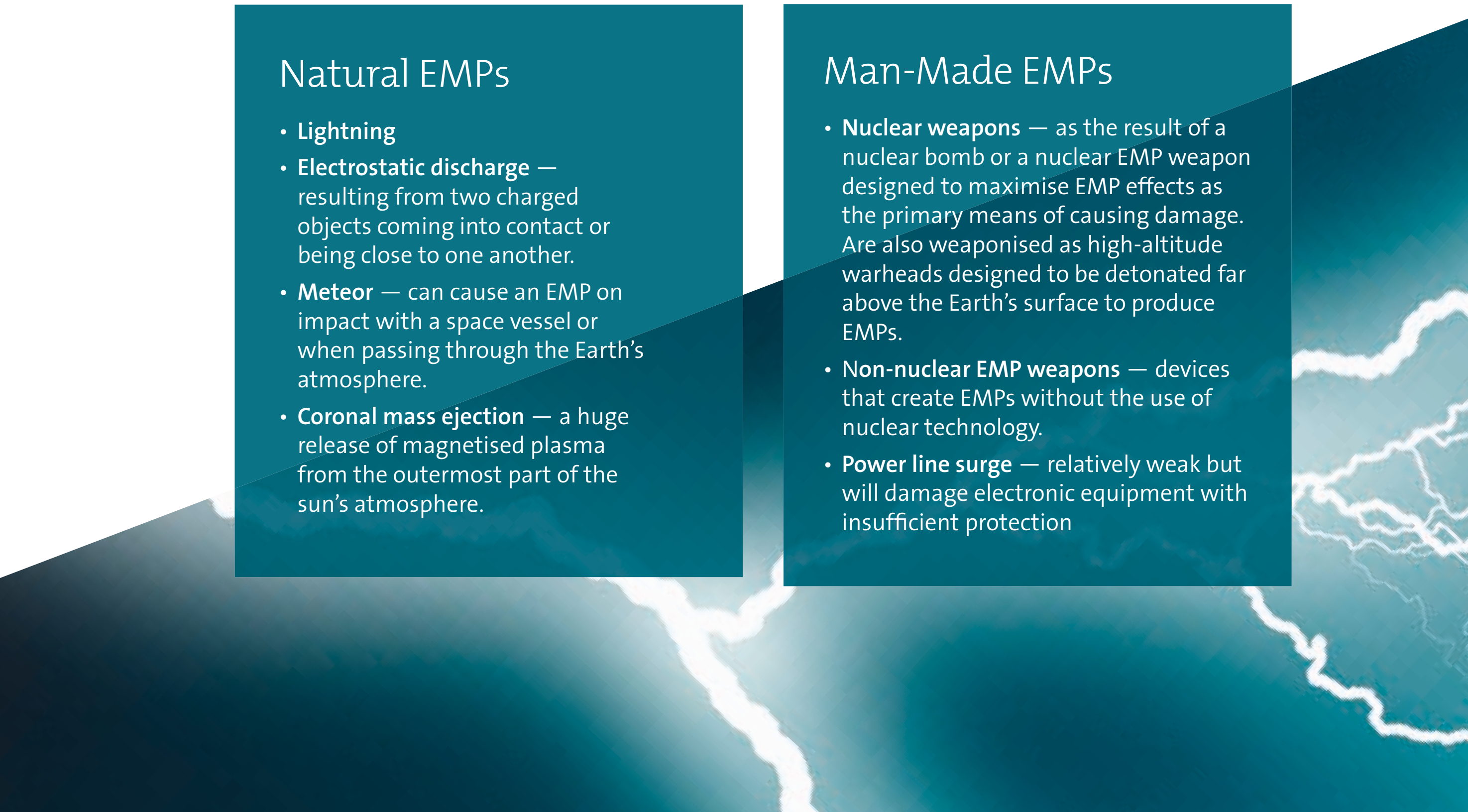
Sources of EMPs

Natural EMPs

- **Lightning**
- **Electrostatic discharge** — resulting from two charged objects coming into contact or being close to one another.
- **Meteor** — can cause an EMP on impact with a space vessel or when passing through the Earth's atmosphere.
- **Coronal mass ejection** — a huge release of magnetised plasma from the outermost part of the sun's atmosphere.

Man-Made EMPs

- **Nuclear weapons** — as the result of a nuclear bomb or a nuclear EMP weapon designed to maximise EMP effects as the primary means of causing damage. Are also weaponised as high-altitude warheads designed to be detonated far above the Earth's surface to produce EMPs.
- **Non-nuclear EMP weapons** — devices that create EMPs without the use of nuclear technology.
- **Power line surge** — relatively weak but will damage electronic equipment with insufficient protection



DAMAGE TO ELECTRONICS AND DATA SYSTEMS

EMPs have a crippling effect on the circuits we rely upon in modern electronics.

All forms of electronics — in fact anything that is powered by an electrical transmission — which are not given the right protection, are effectively rendered useless by an EMP.

As the powerful pulse passes through a metal object, like a phone, computer or server, a "rogue current of electricity" is produced which disrupts or destroys the circuits within.

Furthermore, according to Business Insider, "the power grid, phone and internet lines, and other infrastructure that uses metal may also be prone to the effects, which resemble those of a devastating geomagnetic storm".

Here an electromagnetic pulse can cause power transmission or telecommunications equipment to overload and fail.

HOW SERVER SAFES PROTECT AGAINST EMPS

It is possible to install IT cabinets or server safes which shield servers from the irreparable damage an EMP causes.

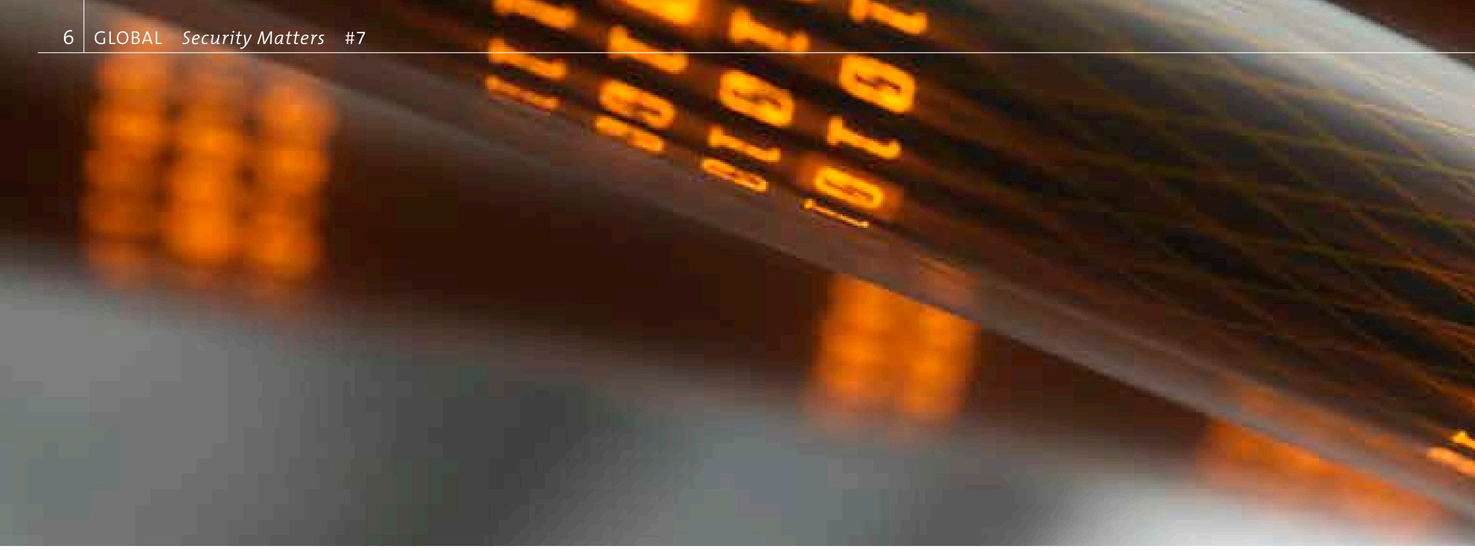
These effectively work as a Faraday cage. A Faraday cage, named after 19th century English scientist, Michael Faraday, is simply an enclosure which blocks electromagnetic fields.

When installing such a cabinet or server safe, make sure it is officially and independently certified for EMP protection. This means it is constructed in such a way as to cancel out the effect of the EMP's field and prevent attached electrical cables from failing.

ADDITIONAL BENEFITS OF EMP SAFES

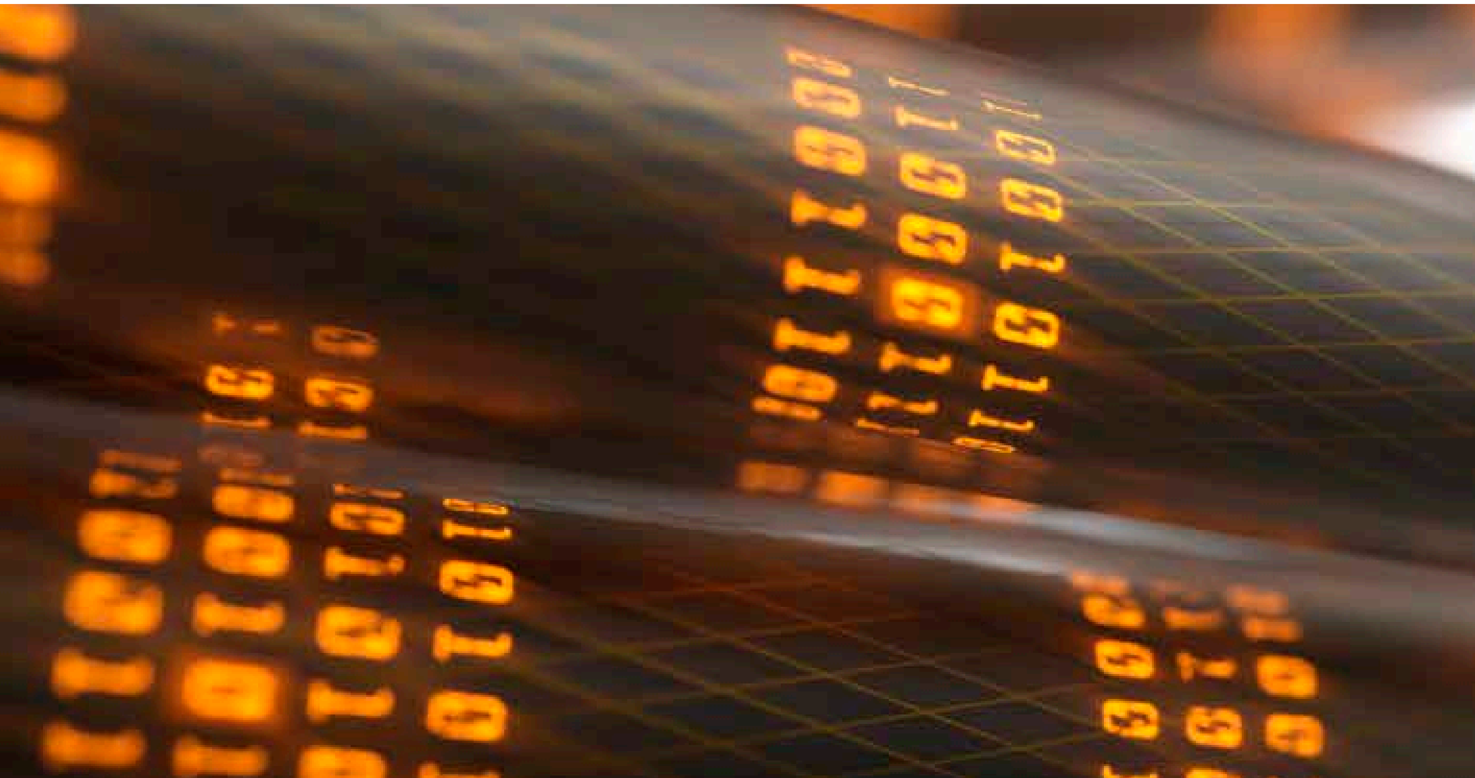
Safes or cabinets which negate the effects of an EMP coming from outside have an added advantage. They also prevent the electromagnetic signals which are generated by electronic equipment from being detected.

This helps in the battle against industrial espionage and so-called "signals intelligence" — a way of stealing information by remotely intercepting the electromagnetic signals emitted by a server.



ANSSI Certification

What It Means for Access Control Systems

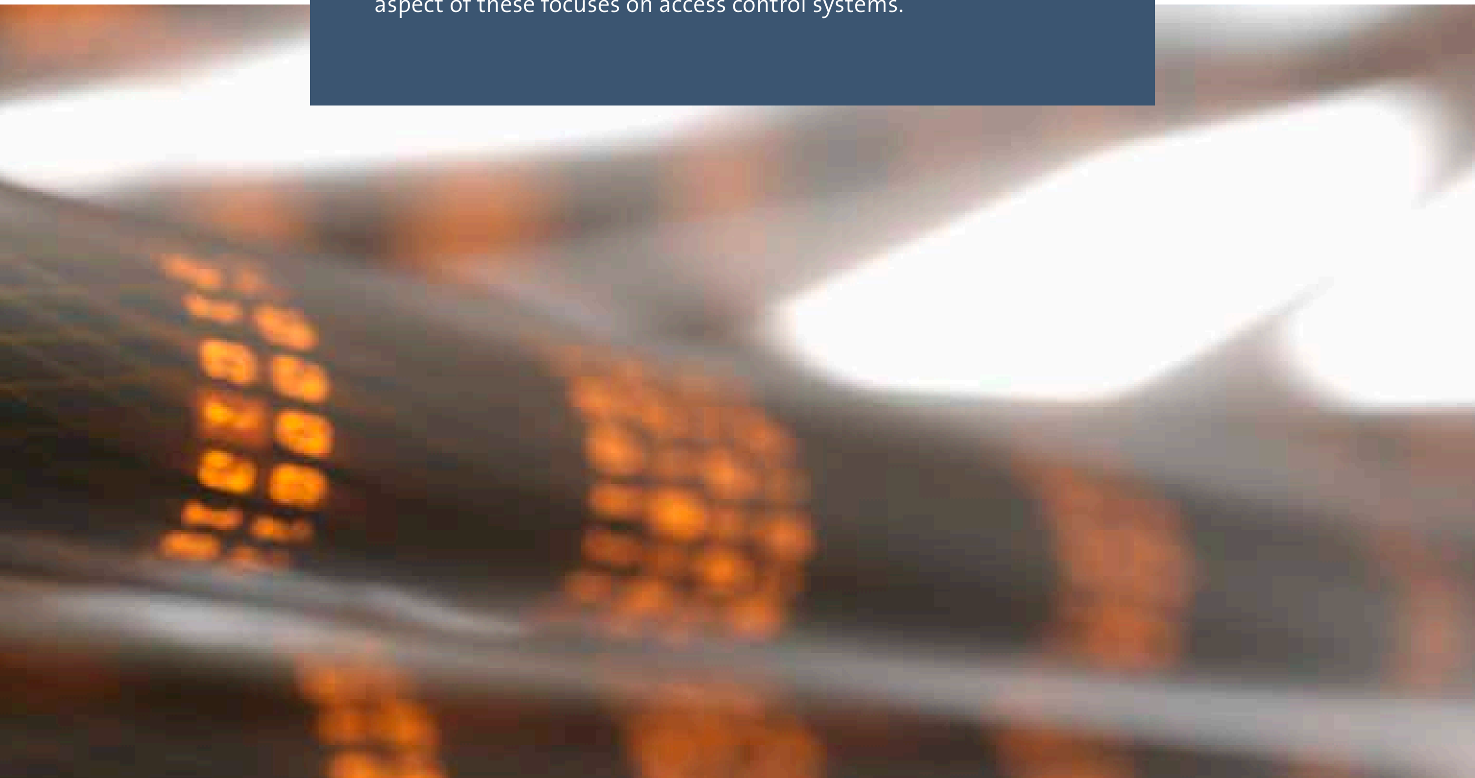


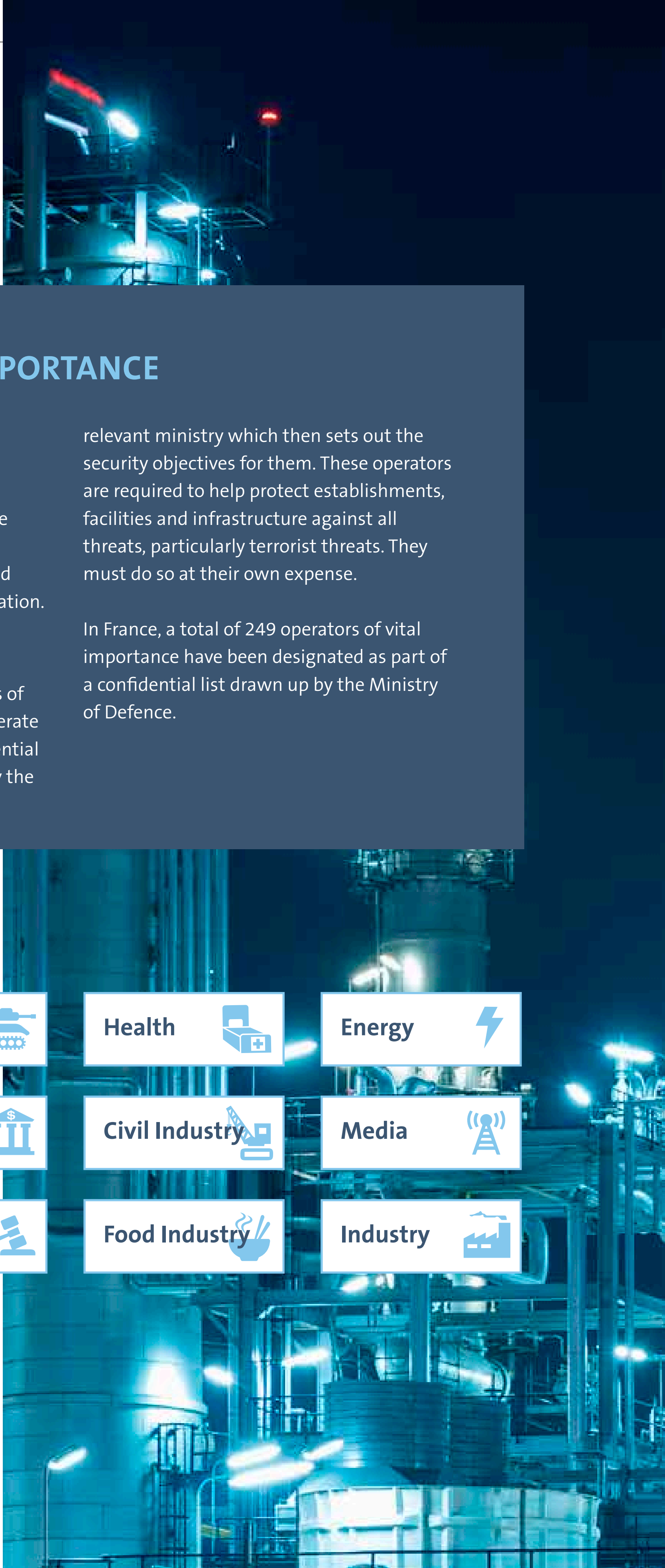
WHAT IS ANSSI?

ANSSI stands for the Agence Nationale de la Sécurité des Systèmes d'Information – France's national cybersecurity agency. It was created in 2009 and reports to the Secretariat-General for National Defence and Security (SGDSN) to assist the Prime Minister in exercising his responsibilities in relation to defence and national security. ANSSI currently serves as France's national cyberdefence body for protecting sectors that are considered of vital importance.

WHY IS THIS RELEVANT?

France is the first country in the world to use regulations for developing an effective cybersecurity system to protect critical infrastructure. It is expected that these regulations could be used as a template by other countries in Europe and possibly beyond. ANSSI is tasked with setting out rules for the protection of information systems and ensuring that the measures adopted are properly applied. These obligations apply first and foremost to information systems that are considered of "vital importance". One aspect of these focuses on access control systems.





SECTORS OF VITAL IMPORTANCE

France has identified 12 sectors of vital importance. These sectors are defined as carrying out essential activities that are difficult to replace. They relate to the production and distribution of goods and services the absence of which would constitute a serious threat to the population.

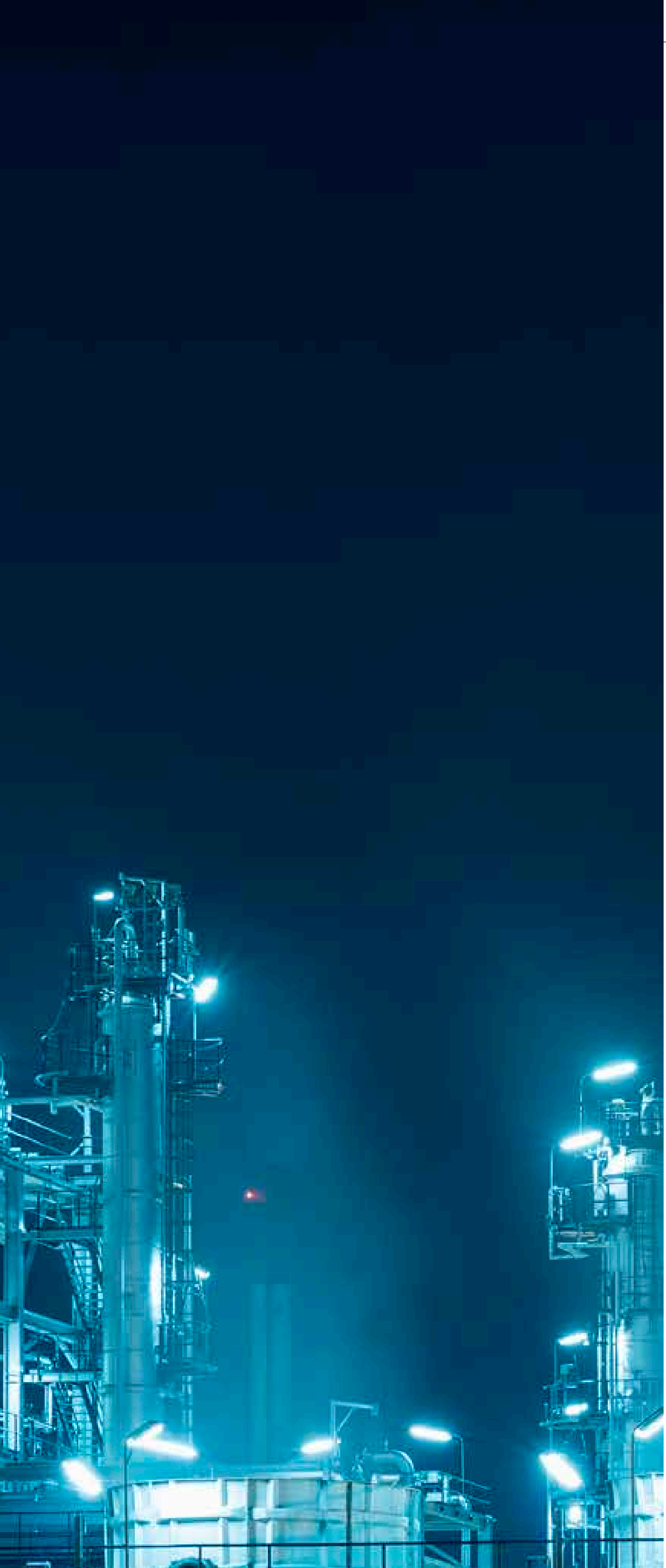
Operators of vital importance

In sectors of vital importance, operators of vital importance are the ones which operate or use facilities that are considered essential for the country. These are designated by the relevant ministry which then sets out the security objectives for them. These operators are required to help protect establishments, facilities and infrastructure against all threats, particularly terrorist threats. They must do so at their own expense.

In France, a total of 249 operators of vital importance have been designated as part of a confidential list drawn up by the Ministry of Defence.

Operators of vital importance by sector

Transport	Military	Health	Energy
Water	Finance	Civil Industry	Media
R&D	Legal	Food Industry	Industry



Locations of vital importance

Locations of vital importance are centres, facilities or infrastructure which provide services and goods which are considered essential for the country.

The operators themselves draw up lists of their locations of vital importance. These can include, for example, production sites, testing centres, network nodes, IT centres, etc. An operator of vital importance can have several locations of vital importance.

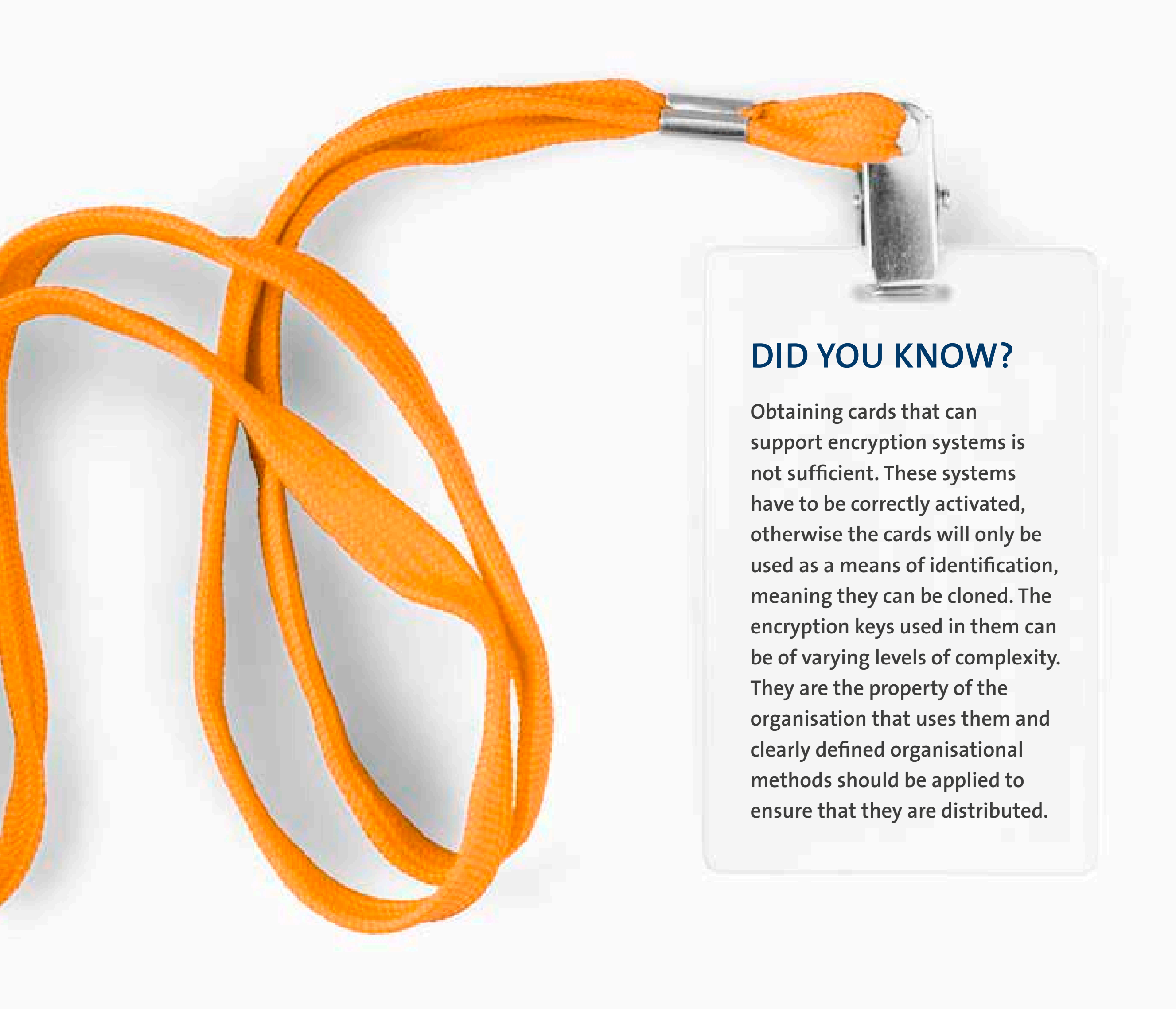
Where several locations are based in the same area, this region is described as a geographic zone of vital importance.

ANSSI RECOMMENDATIONS RELATING TO ACCESS CONTROL SYSTEMS

As far as physical access control systems are concerned, ANSSI has compiled its recommendations in one document, “Guide to the security of contactless technologies for physical access control systems”.

The fundamental principles described in this document are designed to be directly appropriate for the threat levels for each zone, based on the type of potential attack according to a scale ranging from I to IV.

To provide Levels II to IV as recommended by ANSSI, cards with read/write chips are required. Using chips that are certified as meeting common criteria EAL 4+ provides additional security guarantees. The Mifare DESFire EV1 card has established itself as the leading card in this area.



DID YOU KNOW?

Obtaining cards that can support encryption systems is not sufficient. These systems have to be correctly activated, otherwise the cards will only be used as a means of identification, meaning they can be cloned. The encryption keys used in them can be of varying levels of complexity. They are the property of the organisation that uses them and clearly defined organisational methods should be applied to ensure that they are distributed.

The 4 levels of security for protecting IDs

Level I

The card's identification does not use any cryptography: 125 kHz transponder, ISO-14443 card UID. The ID is unencrypted and is therefore easily cloneable. This level has no security guarantees.

Level II

Access to the card's ID is protected with a key so it can be authenticated. Authentication involves a key that is shared by all cards. This is the first level of security: in the event of the key being corrupted, access to all IDs will be rendered possible.

Level III

Access to the card's ID is protected with a key so it can be authenticated. Authentication involves using a key derived from a master key. If one of the keys is corrupted, the other cards are unaffected.

Level IV

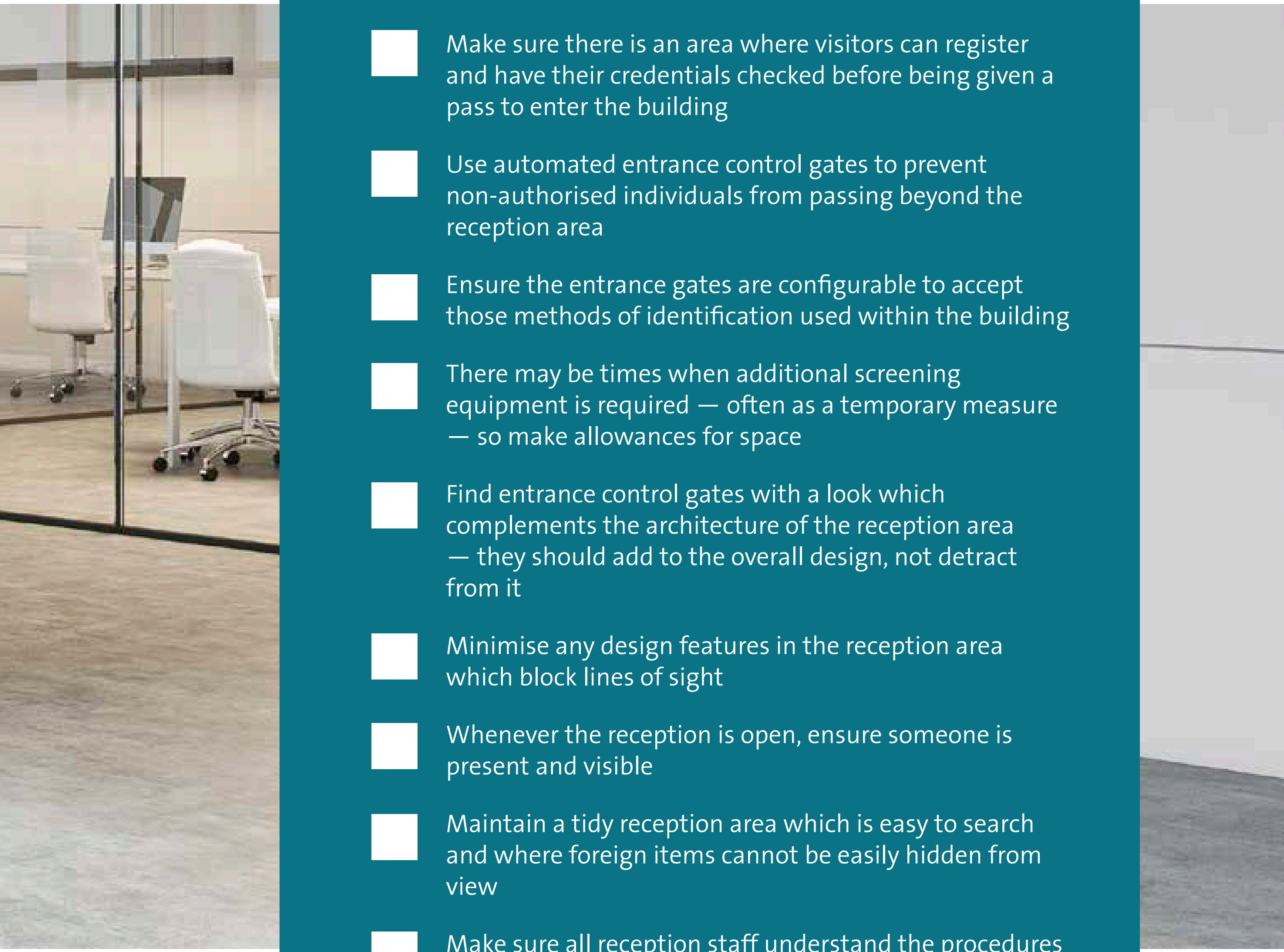
The same as Level 3 + authentication of card holder when they enter a code they have memorised or using biometric data.

ENTRANCE SECURITY

Checklist

How to Eliminate Security Gaps at the Front Desk

As well as creating that significant first impression, reception areas play an important role in office security. But is your front desk up to the job?



Reception Security Checklist

- □ Make sure there is an area where visitors can register and have their credentials checked before being given a pass to enter the building
- □ Use automated entrance control gates to prevent non-authorised individuals from passing beyond the reception area
- □ Ensure the entrance gates are configurable to accept those methods of identification used within the building
- □ There may be times when additional screening equipment is required — often as a temporary measure — so make allowances for space
- □ Find entrance control gates with a look which complements the architecture of the reception area — they should add to the overall design, not detract from it
- □ Minimise any design features in the reception area which block lines of sight
- □ Whenever the reception is open, ensure someone is present and visible
- □ Maintain a tidy reception area which is easy to search and where foreign items cannot be easily hidden from view
- □ Make sure all reception staff understand the procedures for security in that area and know how to act in the event of an emergency

RETAIL SECURITY

Internal Theft and How to Tackle It

Shoplifting carried out by employees – internal theft – is a problem which retailers often overlook. But there are some simple ways to make sure it never happens.

Many countries are seeing a rise in internal theft. Experts point to several key contributing factors for this rise.

According to loss prevention specialist, Luiz F. Sambugaro, these factors make internal theft just as big an issue as external theft. Luiz is based in Brazil where he is a member of several important retail associations.

"What we observe in Brazil, as well as in countries like the United States, is the continual growth of internal theft. A catalyst for this has been the economic crisis which has led to lay-offs, downsizing, outsourcing of labour, and the exchange of trained, loyal members of staff for new cheaper employees with no commitment to the company.

"And there are other contributing factors, such as the cutting of benefits and reduction of maintenance expenses, which are only serving to increase the rate of internal theft.

"Without strategies to curb these crimes, the rate will continue to grow."

REASONS FOR RISING INTERNAL THEFT IN RETAIL

- Tough economic conditions leading to lay-offs, downsizing and outsourcing of labour
- The exchange of trained, loyal members of staff for new cheaper employees with no commitment to the company
- The cutting of benefits
- The reduction of maintenance expenses

To tackle fraudulent behaviour by shop staff, retailers can employ the following three tactics:

1 *Build Staff Loyalty*

One way to reduce the rate of internal theft is to establish a working environment which creates a culture of loyalty and makes employees feel part of a team.

Open communication and clear goals are often the key to creating ownership, as all employees feel they are working towards the same goal.

Working in a place where you are part of a community raises staff's morale and is likely to prevent internal theft – it is better to reward than punish.

2 *Do Not Skimp on Maintenance*

Reports by former thieving employees show that a lack of maintenance is a factor that favours internal theft.

For example, whereas the presence of a camera or product alarm system may be enough to deter a shoplifter, employees know when those systems are faulty and can exploit the lack of action taken to repair them.

3 *Recruit Wisely*

Do not just consider a candidate's professional capabilities when recruiting, but look at their past conduct.

And when you have recruited, make sure all employees have adequate training on both the security systems you have in place and how to actively prevent shoplifting.

CONTACTS AND INFO

THE GUNNEBO GROUP

Gunnebo is a global leader in security products, services and solutions with an offering covering cash management, safes and vaults, entrance security and electronic security for banks, retail, mass transit, public & commercial buildings and industrial & high-risk sites.

We make your world safer.

FIND US

Products and Solutions
www.gunnebo.com

Security Matters Blog
blog.gunnebo.com

Investor Relations
www.gunnebogroup.com

ADDRESS

Gunnebo AB, P.O. Box 5181, 402 26 Gothenburg, Sweden

E-mail: info@gunnebo.com
Tel: +46 10 209 5000

RESPONSIBLE PUBLISHER
Karin Wallström Nordén
SVP Marketing & Communications
+46 10 2095 026
karin.wallstrom@gunnebo.com

EDITOR AND CONTRIBUTOR
Rob Suddaby
rob.suddaby@gunnebo.com

TRANSLATION
Comactiva, www.comactiva.se

PRODUCTION OF LANGUAGE VERSIONS
Newsroom, www.newsroom.se

PRINTING
Larsson Offsettryck, www.larssonoffsettryck.se
Images from Bigstock and Gunnebo.