An Original

Article

Access Control Points

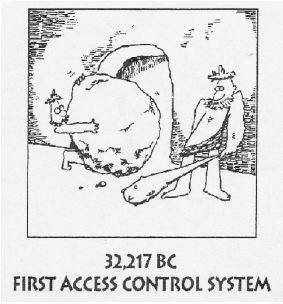
By
Thomas Gordon
Missouri Enterprise Project Manager

Abstract

Access control has two major elements:- physical access and virtual access, which deals with the intellectual property of an organization. In order to provide confidence to Customers [and potential Customers], and the creation of a safe working environment both elements must be adequately addressed.

Access Control [1] is the selective restriction of access to a resource [place, data, and person] to duly authorized personnel. In essence, the methods of access control have not changed over the centuries:

Then



Now [2]

The level of control will, of course, vary according to the particular circumstances of the organization in question – obviously there would be a higher level of control for a factory and its data if the factory was in the nuclear weapon industry than in one that manufactured diaries. However, there are certain

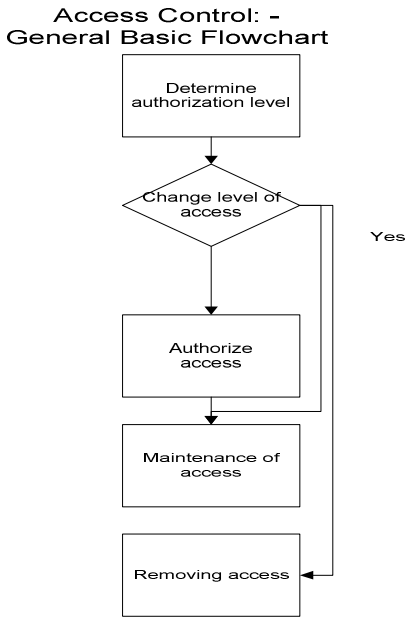
[1] Common synonyms are Entry Control Procedures [ECP] and Unified Facilities Criteria [UFC]
[2] Taken from "A Guide to Nuclear Regulation in the UK", Office of Nuclear Regulation.

underlying principles which are universally applicable – the difference is a matter of degree. Basic to all access control solutions is a comprehensive Access Control manual.

The manual should cover, as a minimum:

- Access Control Policy. This is an explicit statement by Top Management.
    - An example might be:
        - The purpose of this policy is to provide a secure and safe working environment for XXXX employees and to protect the intellectual and physical property of the Customer and XXXX. It is the policy of XXXX that all employees, visitors, subcontractors and vendors follow and agree to abide by the guidelines established in this manual.
- Employee environment
    - Employee screening
    - Weapons policy
    - Leaving policy
    - Personal equipment –especially IOT
- Visitors
- Subcontractors and vendors
- Physical access security
- Cyber access security

A starting point is to determine the requirements of the Customer and determine a 'worst case' scenario. The discipline of FMEA is very effective in determine the degree of risk and implementing mitigation procedures. There is a basic control process, which can apply to all areas of access control:



People

The greatest level of risk is with 'people'; people get blasé about security, people get bored, people are stressed, people get careless and all the other problems that result in the management of an incredibly difficult species. The education and authorization of personnel is a key to effective access control.

As stated above, a good Access Control Policy and comprehensive manual is essential to achieving employee co-operation but only if people are trained and Top Management focuses upon the requirements. Management gets what Management inspects – not what they expect! In security, as well as in all areas of business, this is a truism.

Visitors and subcontractors

Ideally, all visitors should sign in and out, including their vehicle registration number, and be restricted to a Visitors' Conference Room. The safety of visitors, when on site, is often overlooked, especially for 'regular' visitors.

Particular attention should be paid to:

- The valid reason for the visit
- Areas for Visitors to park vehicles
- Internet of Things – especially devices that can record or take photographs
- White boards and flipcharts that may contain proprietary information
- Visitors should be accompanied at all times by a member of the XXXX staff
    - It is often impractical for a subcontractor to be accompanied by an employee, therefore subcontractors should:
        - Have a specific identification badge "**SUBCONTRACTOR**" # 1111
        - Be restricted to their specific area of operation

Physical Security

Physical security is both the most obvious area of control and often the least effective. It is not unusual to find tightly controlled front entrances and then to go around the back of the building to find that the Receiving/Shipping docks are uncontrolled. [There is physical security in anonymity; advertising that you are a supplier to BOEING, for example, may be a red flag to some less than positive people!]

Locks are not sufficient. All a lock will do is act as deterrence to honest people, not someone bent upon mischief. Areas to consider are:

- Security lighting of the area

- Main and visitors' entrance out of hours
- Employee entrances
- Shipping and Receiving docks
- Night access to site
- Access of an employee's family or friends
- Access by vendors bringing in sandwiches or other snacks on a regular basis
- Restricted areas – who is allowed and who is not allowed access

Cyber security

Customer and Company intellectual property, including but not limited to data, samples, forecasts, purchase orders, quotations and specifications, is addressed in ISO 9001:2008 §7.5.4 "Note". "Customer property can include intellectual property and personal data".

Firewalls and virus protection are a given but there is rather more to cyber security than protecting your data against all those nerdy nephews in the hacking business:

- Authorization of access is the purview of Top Management
- All users should have a unique log-on to specific machines and areas of information
- All users must change their passwords regularly, passwords should include alpha-numerics and at least one non-alphanumeric character
- No user should allow others to use their log-on or passwords and passwords should not be written on whiteboards in the office! [3]
- Voluntary or involuntary termination must cause all privileges to be revoked immediately; although it may be too late, so the system should be audited for any issues
- All electronic data should be backed up and off-site at regular intervals. In the event of it being necessary to restore from backups there must be a duly authorized and rehearsed procedure. Restoring data should be part of a Business Continuity Plan.
- All hard-copy documents must be clearly marked and only in exceptional circumstances, with permission, should Customer documents sent electronically be printed. [4]
- Hard-copy communications with vendors or potential Customers should be authorized.
- E-mails should be correctly marked
- Access to non-business related websites should be strictly controlled

This article, by necessity, is a very general introduction to the vast subject of access control, which is an industry in itself. However, by the intelligent application of risk analysis principles

[3] The author of this paper once noticed a list of log-on and password data written on a whiteboard in an area in the World Bank!

[4] See ISO 9001:2008 § 4.2.3 (f)

and practical policies, a comprehensive access control environment can be tailored for any organization and, at the same time, allow that organization to function effectively.

References

Boeing D6-51991, Rev J
Office of Nuclear Regulations, “A guide to Nuclear Regulation”

Unified Facilities Criteria, Security Engineering UFC 4-022-01, 2005. Department of Defense.

ISO 27001:2013 Security Techniques

ISO 9001:2008

Internet of Things, Privacy and Security in a connected world, FTC Staff report, January, 2015
HBR, “*The Internet of Everything”,* November, 2014