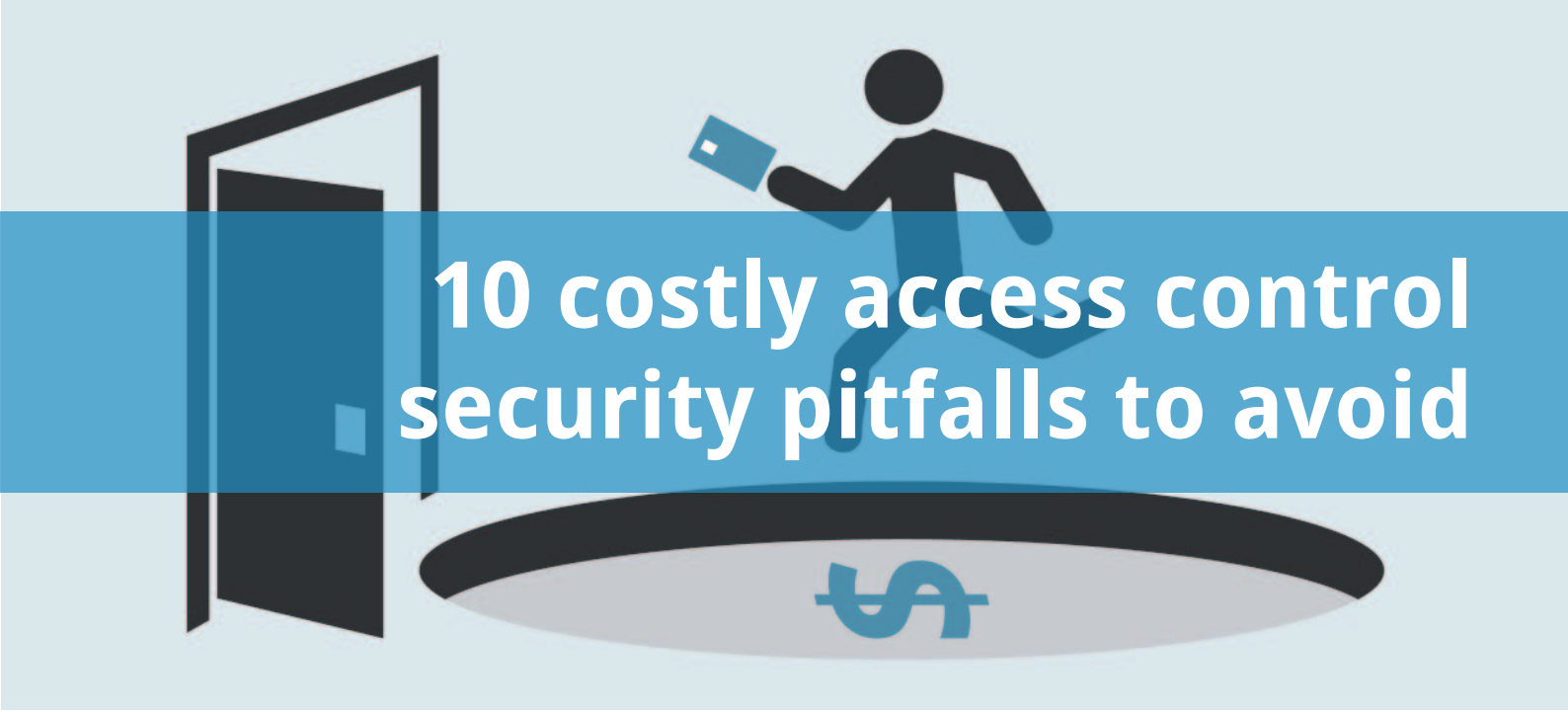

10 costly access control security pitfalls to avoid

Important access control system considerations

→ Using contactless RFID cards to allow secure access to buildings has become the norm, but selecting a physical access control system (PACS) that offers the level of protection expected, and scales cost-effectively, is not as straight forward as you may think.

As well as being aware of the fundamental security gaps to look out for in a PACS, it's also vital to consider the wider integration capabilities that can empower a security system to combat cyber-attacks and insider threats without inconveniencing users.

Because many PACS are proprietary, with limited flexibility and integration capabilities, upgrading them can often be excessively costly or practically impossible. With all this in mind, below are some important considerations to take into account when selecting a PACS:

NO.1 – AVOID HAVING SEPARATE PHYSICAL & IT ACCESS CONTROL SYSTEMS

→ Having a common system for managing user identities across an organisation closes the security gap in staff and contractor on-boarding / off-boarding processes. Removing the need to manually populate and maintain user information in separate databases supports a 'security by default' design to prevent the all-too-common risk from inappropriate continued access:

"36% of desk-based workers in the UK and US are aware of having continued access to a former employer's systems or data"

Infosecurity-magazine.com

→ *For PACS that offer synchronisation with IT access control databases, be sure to understand whether the process is one-way or two-way, how often the data is transferred, and what additional controls may be needed to ensure the privacy and protection of duplicated user information.*

NO.2 – WEIGHT UP THE NEED FOR ONLINE VERSUS OFFLINE PACS OPERATION

→ Online systems respond in real-time to updates made to a user's permissions, making it possible to add new users or rescind rights instantaneously. Offline systems typically take many hours before access right changes are propagated to door controllers, which may hamper staff productivity or create an exposure to risk. Online systems using IP network communications can accommodate different deployment architectures, including data centre, WAN or cloud based, without any degradation in speed or reliability.

NO.3 – CONSIDER THE NEED TO BE ABLE TO MANAGE PHYSICAL ACCESS ACROSS MULTIPLE SITES

→ Some PACS are unsuited to scalable, centralised, management. Site-centric PACS require the addition of dedicated synchronisation appliances to share data between each location on a time-scheduled basis. As well as the cost of these appliances there is a great deal of complexity in managing the sequencing and prioritization of the synchronisation updates, as well as the required communications links.

NO.4 – ASK HOW EASILY THE PACS CAN INTEGRATE WITH IT ACCESS CONTROLS IN REAL-TIME

→ IT access control systems, such as Microsoft® Active Directory, can allow or deny a person's access to any particular IT resource. Direct PACS integration enables the IT access decision to take account of the person's location; requests for access to sensitive data, or to critical systems, from users outside secure areas can be denied. This converged approach to access control combats internal and external threats, as well as supporting increasing compliance needs, such as PCI-DSS.

NO.5 – CONSIDER THE NEED FOR THE PACS TO CONNECT TO AGGREGATING SECURITY APPLICATIONS

→ Consider the need for the PACS, alongside CCTV and alarm systems, to feed data to aggregating security applications which support manned monitoring and event reporting forensics. Aggregating systems include: SIEM (Security Information & Event Management), Security Intelligence, Behavioural Analytics, IAM/PIAM (Identity/Physical Identity & Access Management), PSIM (Physical Security Information Management).

NO.6 – UNDERSTAND THAT SMART CARDS ARE NOT ALL MADE EQUAL

→ Many organisations are unaware they are buying a compromised technology that does not adequately meet their need for protection, because it can easily be copied, cloned or spoofed. Many standard cards are known to be vulnerable, but continue to be sold by PACS providers. Even 'secure' cards are often sold using 'open' numbering schemes that are not unique to each customer, so can be easily, and legally, be replicated.

NO.7 – AVOID CARD TECHNOLOGY 'LOCK-IN'

→ As well restricting competitive supplier choice, lock-in may prevent PACS cards from being used for PC log-on, follow-me printing, and other applications. Converging identity and access management across an organisation with a single ID-card streamlines process and reduces costs, while maximizing user convenience, security and compliance.

NO.8 – SAFEGUARD THE MANAGEMENT OF ENCRYPTION KEYS

→ Even when using secure RFID card technologies, organisations often allow several third-parties in their PACS supply chain access to critical card security data. While organisations are quite rightly unwilling to share their firewall or domain admin password with third parties, many seem oblivious to the potential risks of relying on others to hold securely their smart card encryption keys.

NO.9 – ENSURE THE PACS IS AS RESILIENT AS OTHER CRITICAL IT SYSTEMS

→ Ensure the PACS is able to operate through power outages and has data backed-up ready for fail-over and disaster-recovery use. Ideally, find a solution that leverages existing server and database backup and replication regimes to reduce cost and complexity.

NO.10 – AVOID THE TIME & SIGNIFICANT INSTALLATION COSTS OF EXCESSIVE CABLING

→ Older PACS designs don't use standard IP network cabling and require extensive cable installation. Individual IP-based controllers located near to each door, and powered by PoE, are typically more cost-effective than having large concentrations of hardware in a service cupboard that necessitates additional wiring complexity. PACS that support wirelessly controlled locks minimizes installation effort, with a single IP networked hub securely controlling many wireless locks.