Straight Talk from the Corner Office

CORANET
WE PUT A FACE TO TECHNOLOGY®

Spring 2017

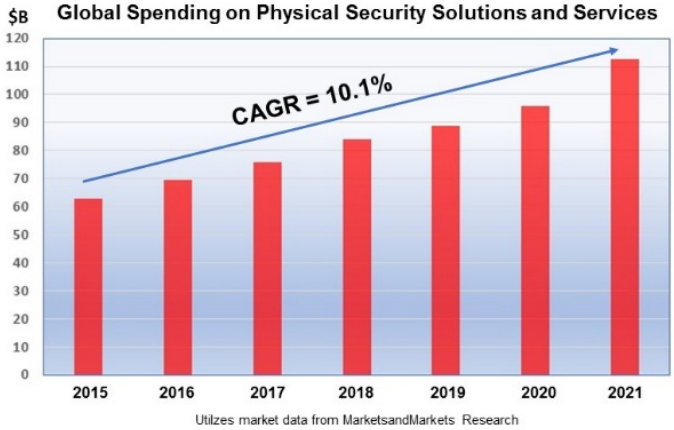
Ensuring the Physical Security of Your Business

Welcome again to *Straight Talk*, one of the ways Coranet shares perspectives on important issues and opportunities in business technology.

Sadly, we are greeted with near-daily reports on the relentless efforts of hackers to penetrate our data networks for financial or political gain. As we have discussed in previous Straight Talks (see Issues 4 and 5), it comes as no surprise that cyber security remains a top-of-mind priority for business leaders worldwide. In this issue, we will extend the data security theme to take a closer look at a related area of growing executive concern – the safeguarding of business *physical* security.

A Cross-Vertical Investment Priority

Although somewhat less headline-grabbing than high profile cases of cybercrime, it's clear that business leaders are increasingly taking physical threats seriously. This can be seen in the expected 10⁺% compound growth of business spending on physical security (seen on the right), which is nearly double the 5.7% CAGR for overall IT budgets, as recently reported by global research firm *IDC*.



Utilzes market data from MarketsandMarkets Research

Geographically, North America leads in physical security spending, with the retail, government, healthcare and hospitality segments showing the highest levels of security-related investments.

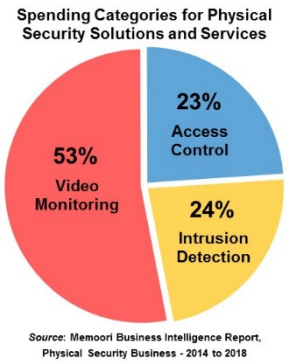
Where are the Threats Coming From?

Although there isn't an agreed-upon centralized database that tracks security breaches, a well-publicized independent study involving 300 business leaders by *Loudhouse Research* found that 40% of the security incidents experienced by the participating firms came from active or ex-employees, and another 18% came from trusted suppliers that had facility access.

The unsettling reality is that a sizeable proportion of perpetrators are individuals that have insider knowledge of building layouts, and are often able to operate unobserved because of their job duties. Clearly, regardless of where the threats are coming from, taking the necessary steps to safeguard your business should be viewed as an essential leadership 'must-do'.

The Basics of Physical Security

All technologies associated with physical security have as their common purpose the protection of a firm's facilities, personnel, intellectual property and capital assets.



Source: Memoori Business Intelligence Report, Physical Security Business - 2014 to 2018

As shown in the diagram on the left, business investment in physical security is divided across three functional categories, with video monitoring out-pacing the spending in building access control or intrusion detection by more than a 2x factor.

Video Monitoring

Also referred to as *video surveillance* or *closed-circuit television* (CCTV), video monitoring utilizes cameras and recording equipment to provide a visual record of activity that is typically focused on building access points, parking lots, loading docks and high-value areas like data centers and communication equipment rooms.

First introduced commercially in the 1970's, early CCTV systems utilized individually powered cameras that captured images in an analog format, and then transmitted them over dedicated cabling to a centralized *Digital Video Recorder* (DVR). Once received by the DVR, the analog signal was converted to a digital format, recorded, and then stored on an internal hard drive for later retrieval and viewing.


Contemporary high resolution IP camera capable of image tracking and zooming
Courtesy: *Axis Communications*

The current generation of IP-based video surveillance systems was introduced in the late 1990's and differs from the earlier approach in several ways. Relying on natively digital rather than analog technology, the image quality of the IP cameras used by the new systems has been dramatically improved, with current IP cameras able to deliver up to 20-megapixel resolution compared to the previous maximum of 0.4 megapixels with analog cameras.

Able to send video wirelessly as well as through existing Local Area Networks, IP cameras not only avoid the need for dedicated cabling, but can also be powered directly through their Ethernet connection – eliminating the need for a separate electrical circuit and greatly simplifying camera deployment.

Two other advantages of IP surveillance systems should be called out. Similar in basic function to the earlier DVRs, IP systems use *Network Video Recorders* (NVRs) that can be equipped with image identification and analytics software that allows the system to automatically analyze images in real time, and alert designated personnel when suspicious activity is identified. This software has recently advanced to a very high degree of accuracy (currently approaching 95%), and can potentially reduce or eliminate the need for security personnel to constantly monitor incoming video footage. The new IP systems are also more scalable than their predecessors – both in terms of being able to support more cameras, as well as allowing utilization of local or Cloud-based storage solutions to provide virtually unlimited video file retention.

Intrusion Detection

Typically deployed in combination with some form of alarming, intrusion detection systems can utilize a variety of devices to address the particular environment being protected – glass breakage detectors for areas with windows, infrared and photoelectric motion detectors that sense unexpected changes in heat and light, and ultrasonic detectors that can register deviations from the normal 'acoustic signature' of a room. Associated alarming can vary from use of so-called *repellent alarms* that use sirens and strobe lights to encourage intruders to leave the area, to *notification alarms* that transmit silent alerts to responsible individuals or 3rd party security monitoring and management services.

Access Control

Generally considered to be the component of physical security that is most frequently 'challenged' by perpetrators, access controls use various techniques to authenticate the identity of individuals and provide them with pre-authorized levels of facility access. Fortunately, the traditional (and easily defeated) photo ID is giving way to more secure technologies, from microchip-embedded smart cards, to biometric devices that validate individual identity based on facial recognition, fingerprints and the unique iris patterns of the eye.

Key Considerations for Physical Security Solutions

Should you decide to move forward with a security system deployment, expansion or upgrade, we have found that the following checklist can be very useful in helping ensure a successful outcome.

The Critical Importance of Planning As with any technology, the effectiveness of security solutions is hugely dependent on careful upfront planning. Typically beginning with a comprehensive vulnerability assessment that identifies credible threats and the likely business impacts from intrusion, the findings enable development of a fact-based plan that allows each business to achieve the right balance of risk mitigation and security solution investment. Be sure to involve all key stakeholders in the planning process – executives, legal, HR and building operations at a minimum.

Security is an On-going Commitment In a strong parallel to the situation with cyber security, the sophistication of physical intrusion 'exploits' is steadily increasing, which means businesses must regularly test their security measures and adjust as needed. Necessary changes can involve modification of security practices as well as technology adjustments. In addition to actively testing your security solutions, a best practices approach also includes tracking of security effectiveness over time through use of performance-based metrics such as the number of successful and unsuccessful intrusions, the percentage of 'false-positives', and the actual financial impact of any security breach.

Engage the Right Support if Needed As a specialized set of technologies, the design, deployment and management of physical security solutions is likely to fall beyond the experience of most IT departments. Many mainstream business communications providers also lack essential security-related expertise, so pay particular attention to a potential provider's security credentials before making your selection of a trusted partner. Since security solutions are often connected to other building management systems like fire detection and suppression, choosing a security partner with skills in office automation can also help ensure a comprehensive and fully integrated approach for your business.

A Final Thought

Although there are a number of good reasons to deploy the newer IP-based security solutions, the fact is that many analog systems are still in active use and don't necessarily need replacement. A well-conducted security assessment will document the effectiveness of existing security assets, and provide guidance on areas in your facility that are well-served by analog systems, as well as those environments where newer technology can provide higher levels of protection. If existing solution components are being retained, a capable security partner will help you integrate analog and IP components for an effective total solution.

Thank you for joining me in our brief discussion on the importance of safeguarding the physical security of your business. If this short overview has intrigued you or brings additional questions to mind, we would enjoy continuing the discussion. As always, I welcome your feedback. Please direct any questions or comments to questions@coranet.com.

Margaret