SECURITY SYSTEMS NEWS
THE SECURITY INDUSTRY'S MOST TRUSTED NEWS SOURCE

ROUNDTABLE DISCUSSION: SECURITY SYSTEM LIFECYCLE CONSIDERATIONS, EFFECTIVENESS AND COST CONTROL

General News

Frank Pisciotta
Updated Fri August 23, 2019

A substantial focus of the security industry is on the selection and installation of security systems, and there is no doubt that this is a critical element of the process.🔲 However, in order to ensure that security systems such as access control, video surveillance, intrusion detection and panic alarms deliver on “game day,” an equal if not greater emphasis has to be put on the actions that are taken after the installers have closed the doors on the truck and driven away.

This article covers some important issues which were covered at the 2019 International

X Dismiss

David Barnard of RS2 security highlighted the importance of backwards compatibility in access control software solutions. Reputable manufacturers are constantly evolving software products and it is critical that software continues to work with all installed hardware or owners will find themselves purchasing equipment a second time, which is never good news. I related a case study with a client where the video management software upgrades were not backwards compatible through the mobile app and a small manufacturing site was looking at a $75,000 price tag to upgrade cameras to make them compatible with the “updated software.”

Jim Primovic from Assa Abloy cautioned about the risks of failures in door hardware products resulting in a failure to attention to detail in the selection and, in particular, the installation process. He explained the importance of using certified installers to avoid operation problems.

In light of constantly evolving software revisions, how often do you see any additional training provided to end users when software updates are released?[illegible] Not often in our experience. Charles Johnson of Open Options raised this important point and it is an excellent one. As organizations think about structuring maintenance agreements, it might be wise to consider ongoing training to cover software updates and ensure that end users can continue to optimize the features and benefits of software revisions.

Kim Kornmaier of Honeywell mentioned another element of security system lifecycle consideration: software support. Maintenance agreements are available and will likely be offered from every installer and come in a variety of flavors. I cautioned that care needs to be exercised to ensure that whatever services and support are included in the scope of a maintenance agreement have a clear correlation between service and software upgrades versus the fee charged.[illegible] Maintenance agreements should be avoided that simply guarantee the free replacement of parts (which may or may not ever get used, even after you pay for it). Services you might consider including would be software upgrades, system testing and replacement of consumable parts, like back up batteries.

Another key issue ties directly to periodically measuring and ensuring the risk reduction results of your system. For example, with an access control system, there are several actions recommended for system owners:

Conduct periodic door and alarm testing. (This presumes you have installed all of the

X Dismiss

and all alarms should be investigated to determine root cause and corrective action needed. Organizations who fail to harness door alarming capability are giving away up to 50 percent of the system's potential benefit.

Ensuring the integrity of the access control database. The failure to manage this can lead to unauthorized access and serious security incidents. This can be achieved in a variety of ways, but in the majority of risk assessments we have conducted over the years, it is common to find separated employees and contractor records with active credentials in the database. Ways to mitigate this risk include:

- Integrating your access control database with active directory (works for employees, not so well for contractors);
- Utilizing expiration dates on contractor credentials;
- Periodically manually auditing contractor and employee active badge reports for anomalies, which may indicate process weaknesses in the change management process;
- Utilizing the “use it or lose it” feature in many software programs that automatically disable a credential after a set period of non-use (e.g., 90 days); and
- Establishing processes to limit the removal of certain badges from the site (e.g., those issued to contractors or temporary employees).

Irregular schedules, holidays and natural disasters can result in access vulnerability. For instance, if access-controlled doors at a site are programmed to open on a timer and something prevents persons from arriving at work (e.g., snowstorm), a site may be left exposed. A mitigation against this type of risk would be to employ a concept called “first card unlock.” Under this feature, a lobby entrance to an office, for instance, would not enter into an unlocked state until the first authorized employee presented a card and entered the workplace.

Holiday programming in some systems needs to be changed on an annual basis.🔲 Managing holidays in an access control system results in doors staying secure which would otherwise be unlocked on a normal business day.

Similarly, intrusion detection, duress devices and video surveillance systems can let you down without the proper care and feeding. Examples would include:

X Dismiss

- A panic device fails to communicate an emergency situation because it was not properly reset or the wiring has been damaged due to poor installation. Panic devices should be regularly tested and ideally the activation during testing should be by a person who would be required to use the device in an actual incident. The objective here is to build competency in the persons who may need to activate a device discretely. Similarly, intrusion detection systems should be carefully tested to ensure that all devices are properly reporting to the panel and that the panel is communicating properly to the central station. If there are redundant communications channels, each should be verified.
- In the same way you would conduct audits of active credentials in an access control system, it is strongly recommended that you perform a similar review with PIN codes which have been assigned and would allow for an unauthorized person to disarm a system.
- Utilizing the failure-to-close feature to ensure that through collusion or negligence, if the last person out of a restricted area fails to arm the panel, the central station will notify a responsible party about the omission. Further, reviewing opening and closing reports might well detect inappropriate entries by authorized personnel which are indicative of suspicious or illegal activity. These features and reports will likely be at an additional cost, but they are important insurance to protect against insider threat.
- It is not uncommon to hear about an incident happening and during the investigation, the owner of the system discovers that the needed camera was not recording. Where video is not under routine observation, it is recommended to determine if your video management system can send an alarm in the event of video loss. This would allow for rapid remediation before the video loss is discovered in the course of an investigation.

With respect to video surveillance, as systems grow and evolve over the life of the system, organizations may experience degradation. Darren Giacomini of BCD has studied this issue extensively and concludes that in many cases, installers or others are simply putting too many devices on a VLAN which results in latency and other conflicts.

Degraded video quality has a finite number of potential root causes. In almost every case, degraded video quality is directly related to resource saturation. The resources on a surveillance network consist of IP cameras, network switches, network uplinks, viewing stations, database management and archivers. According to Giacomini, each of these resources share a common thread. And, at the basic level, each of those items are nothing more than a purpose-built computer with limited CPU, memory and network capacity. When any of these resources exceed their capacity, the quality of service delivered will degrade. The following are common

X Dismiss

- IP camera CPU utilization is in excess of 85 percent;
- CPU elevation in the decoder or workstation decoding the video; and
- Network congestion or CPU elevation in the network switch.

Giacomini indicated that the majority of the time degraded video is associated with resource depletion in one of these key components. Investigation of the potential causes above can save time and effort, and prevent a video management software application from unduly being blamed for poor performance during its lifecycle.

Also, on the topic of video, John Kampfhenkel of Veracity discussed the challenges that organizations face when video management system storage is undersized and the need to carefully plan for video retention of existing recorded data when the video system has to be expanded. This can be a problem organizations face and when they do, it is best to involve a video storage expert to determine options, costs and potential legal requirements for maintaining the integrity of archived video data.

Dependent on the level and type of integration between various systems, another challenge may be to preserve the integration between the two systems. System owners will need to coordinate carefully with your installer(s) to ensure that a software revision to one system will not result in a disruption to a software level integration. This type of integration may require a delay in being able to upgrade one or the other application software versions until the integration can again be certified.

Selecting the right security technology is an important element of an organization's security risk management. However, we would argue that in terms of getting measurable results from technology, there needs to be a keen focus on sustaining activities after the installer closes the doors and drives away. By adhering to the consultant and manufacturers' guidance in this article, organizations can substantially reduce the risk to people, assets and information, and prevent criminal and terrorist incidents in the workplace.

Frank Pisciotta, CSC, is president of Business Protection Specialists, Inc., a nationwide independent security consulting firm focused on healthcare risk identification, regulatory compliance and security design services. Pisciotta has managed more than 4,500 security-consulting engagements in his thirty-year consulting career. He possesses a master's degree in public administration, a bachelor's degree in criminal justice and was board certified in Security Management by the American Society for Industrial Security as a Certified Protection Professional in 1994. Pisciotta serves as the Vice Chair on the ASIS Council for Food Defense and Agriculture Security. He can be reached at fp@securingpeople.com.

X Dismiss

access control, ASIS, Business Protection Specialists, Frank Pisciotta, IAPSC, International Association of Professional Security Consultants, intrusion detection, panic detection, video surveillance

Comments

To comment on this post, please log in to your account or set up an account now.

X Dismiss

Need the Latest Security News in the Industry?

Want to always have the latest security news in the industry right in your inbox? Click the button below to subscribe.

SUBSCRIBE NOW

SPONSORED STORIES

WeSuite's Tracy Larson Shares How Speed and Accuracy Grow Sales Organizations
By WeSuite

Four Ways Your Sales Process Defines Company Growth & Profitability
By WeSuite

X Dismiss

By WeSuite

From Forty Hours to Forty Seconds: WeSuite Helps SAGE Integration Automate Bid Submissions and Win More Projects

By WeSuite

Categories Recent Archives

Commercial

Monitoring

Residential

Suppliers

Cybersecurity

General News

Also Noted

On The Editor's Desk

Monitoring Matters

20 Under 40

40 Under 40

Fire Systems Installation

News and Notes

X Dismiss

RELATED ARTICLES

Axis Communications opens “Space City” experience center

CHELMSFORD, Mass. – Swedish security device manufacturer Axis Communications has recently celebrated the opening of their new “Space” themed experience center in Houston, Texas. The Houston Axis Experience Center (AEC) will be Axis’ 13th experience...

Read Article →

Sentinel Consulting names security veteran George Anderson as Senior Advisor

NEW YORK—Sentinel Consulting, a full-service security consulting firm that advises high-profile, high-net-worth clients in the areas of security management, law enforcement, emergency services, and security technology, announced that George W. Anderson has joined the company...

Read Article →

Nice/Nortek Control launch line of linear surveillance cameras at ISC West

CARLSBAD, Calif.—Nice/Nortek Control is set to showcase their brand-new smart and AI powered intelligent Linear Surveillance Cameras and Network Video Recorders (NVR) at ISC West 2022. This multi-family cameras and NVRs are designed to seamlessly integrate with Linear Access

X Dismiss

ABOUT US

OUR TEAM

ADVISORY BOARD

CONTACT US

MEDIA KIT

ADVERTISE

ADVERTISER DIRECTORY

X Dismiss

X Dismiss

Lowest Cost FACP Solution
with Built-in Cell Reporting
NAPCO
FireLink FACP
FACP w/Cell
from
$400 net
StarLink
Cell Up
Inside