Originally Published on SecurityInfoWatch.com

Why Self-Test Health Checks Aren’t Enough

IT-Class Systems Management for Physical Security Systems

Selected excerpts from the original article.

By Ray Bernard, PSP CHS-III

The State of Security Systems Management

To understand the state of *systems and network management* for electronic physical security systems, in contrast with that of IT practice, it is important to take a little historical context into account.

In the 1980’s and ‘90s, networking grew, and network uptime became important. In the 2000’s, networked real time information systems became the backbone of business, and network uptime became *critically* important. Today, it remains an absolute business necessity.

IT can’t wait for network or system failures to occur. IT has to be highly proactive, getting out in front of problems before they become disasters. And IT has to be as predictive as possible, by watching the performance indicators of equipment and applications, to keep their organization’s information systems running smoothly.

IT achieves 99.999% uptime across a mix of multi-vendor, multi-application computing infrastructure. So can Security.

Today, businesses are using *advanced analytics* to get end-to-end insight across their entire information systems infrastructure. Meanwhile, security directors and managers still have security officers scrolling through video camera displays in an attempt to ensure system integrity. It’s not effective, because even if a camera is “on” it does not mean it is recording. Back in the 20th century, with analog technology, officers had to visually inspect camera status *because there was no other option*.

Today, it's a different story. Advanced IT monitoring and management technology can check all devices and systems 24/7. Personnel are notified instantly of a component failure, or of a near-failure condition, and have diagnostics information at their fingertips.

Yet, security departments with 21st century security technology are still applying 20th century management practices. Neither security departments nor their systems integrators have end-to-end insight across their entire security systems infrastructure. So it can happen that video stops recording or retention periods fail to be met and nobody knows.

In spite of video management software self-test health-checks, investigators still find critical video missing.

This needless compromise of security's mission stems from one single fact: The security industry lags years behind in *information technology practices*. Thankfully, this is a simple problem to fix: *adopt the sensible practices of IT infrastructure management.*

You wouldn't buy a new car (in fact you couldn't even find one) that doesn't have a comprehensive computerized diagnostics system built into it, and you wouldn't take that car to a service center that didn't have a separate computer system to read the diagnostics data and analyze the car's systems in real time while it's running. That's the state of technology today.

Individual self-test health-checks do not tell you what you need to know, when you need to know it.

Why remain a decade behind, and accept a security systems infrastructure that doesn't have IT-class systems and network management technology as part of its build-out?

Self-Test Health-Checks Only Work on a Single Vendor Basis

Prior to networking, when security systems were standalone systems, there were no shared infrastructure elements. Today, security systems are much more complex, share a common network infrastructure, and contain software and hardware components from a variety of manufacturers. Each product can check and report on what it knows about itself, but can't report much, if anything, about the remainder of the infrastructure.

This is especially apparent with regard to video surveillance systems. If not all of a camera's video stream data is getting through to the video server or its storage server, there can be any number of reasons for that problem that have nothing to do with the camera itself or the video server.

Today's sophisticated applications also have a certain degree of fault-tolerance, which is why video management system software can continue to record video even when some of the video frames are not successfully transmitted. This is one reason why not all problems are visible on-screen. It takes automated technology to detect this kind of problem. Without comprehensive performance and diagnostics information for the entire infrastructure, there is too little information for troubleshooters to go on, especially for intermittent problems.

Taking a step back, one can see other factors involved in why self-test health checks fall short.

Self-test health checks remain narrowly focused because no vendor will invest in making his competitors' products and systems run better. Additionally, each product is focused on its own functions. It's not looking at what happens between itself and the other vendors' products and systems that it interacts with. This is why 3rd party technology (i.e. something outside the physical security systems themselves) is required for infrastructure management. This is true not just for video, but for all of the security systems technology.

These are just some of the reasons why IT doesn't rely on self-test health checks to manage its information systems technology. Now that security systems are based on information technology, we shouldn't either.

These are just some of the reasons why IT doesn't rely on self-test health checks to manage its information systems technology. You shouldn't either.

Using IT-Class Technology Infrastructure Management

A 21st century automated approach to security systems management makes a big difference in system and device uptime. Here are some of the differences between the current common state security industry practices and current IT practices, and the results of applying the IT practices. *Note that there are a few industry leading companies who already do apply IT practices and make maximum use of service management tools; however, they are the exceptions.*

Infrastructure Documentation

- **Industry Practice:** Most security systems are poorly documented if at all; network documentation often exists but is rarely consulted; cable labeling follows no particular standard and if done, deteriorates over time.
- **IT Practice:** Infrastructure documentation is produced by comprehensive automated discovery and is kept up to date; equipment and application configurations are well-documented; cabling and other physical infrastructure elements are permanently labeled according to common practice and organization standards.
- **Result:** Service work is accurate (no configuration guessing) and no time is wasted figuring out what connects to what; service costs are reduced and repair times are shortened.

Finding Problems

- **Industry Practice:** Some trouble symptoms are randomly discovered by end users.
- **IT Practice:** Automation finds not only symptoms but also root causes
- **Result:** Instant problem detection occurs plus early warning for situations near their problem threshold

Assessing Problems

- **Industry Practice:** Guesswork and past experience are used, there are limited diagnostic tools
- **IT Practice:** Scientific analysis utilizes complete infrastructure knowledge and real-time status information.
- **Result:** Rapid root cause identification, drastically reduced troubleshooting time, and elimination of needless truck rolls for troubleshooting are achieved, resulting in much greater service capacity per technician.

Diagnostic Information Storage

- **Industry Practice:** What little information that is collected is stored on the system's own server, requiring server access for problem troubleshooting; data is lost if the system dies, data is inaccessible if the application crashes or the intelligent device is offline or had died.
- **IT Practice:** Diagnostics information is centralized outside of the monitored systems, and is also backed up in the cloud (a growing trend).
- **Result:** Direct access to the critical system is not required for diagnosis; if the system or device fails the troubleshooting information is still available.

Corrective Action Plans

- **Industry Practice:** Fix-it actions are performed ad-hoc based upon end-user or systems integrator experience.
- **IT Practice:** Corrective and preventive action planning is based on automated root cause analysis supported by a comprehensive technology knowledgebase
- **Result:** Corrective actions *actually are* correct and thus permanent; the technology knowledgebase is enhanced; preventive measures improve uptime even more.

Informing the Team

- **Industry Practice:** Ad hoc phone calls, emails and text messages are used; notifications to stakeholders are inconsistent and insufficiently informative; high level access passwords are shared insecurely for systems and devices (plus integrators commonly use master passwords used across a wide customer base); diagnostic information with sensitive data is often over-shared and ends up residing in poorly secured outside computers.

- **IT Practice:** Automated stakeholder notifications are performed instantly with message content appropriate to the stakeholder's role; **alerts** (failure or critical problem), **warnings** (failure likely) and **advisories** (performance below par) with appropriate diagnostic information enable support teams to be maximally proactive and to correctly assign and prioritize service tasks; automated service management tracks workflows and escalates stale task completions.
- **Result:** Service work dropped balls are eliminated; system downtime is minimized; team members are optimally utilized; customers are kept fully informed; and service is highly efficient and very cost-effective.

Collaboration Technology

- **Industry Practice:** Telephone conference calls and desktop sharing technologies are used; remote access to live systems is used and sometimes shared (such as LogMeIn or TeamViewer) and is usually not logged or tracked (end-user customer may have no knowledge); industry practice around remote access security is very poor; collaboration is often sequential (one vendor or service provider at a time); lacking hard diagnostics data, conference calls often result in finger-pointing.
- **IT Practice:** Purpose-appropriate collaboration technology is used to securely share diagnostics information; remote access to live systems is limited to authorized technicians making corrections; all systems stakeholders share the full scope of diagnostics data (technology vendors, technology service providers, in-house network personnel, and end user).
- **Result:** All parties are fully informed with good diagnostics data; finger-pointing is eliminated; collaboration time is shortened for all parties; and no diagnostic information resides outside the customer organization's data repository.

Conclusion

Self-test health checks don't provide the kinds of results listed above. There is real Return-On-Investment in the IT practices, which that security industry Self-test health checks just can't deliver.

Management, compliance officers, financial stakeholders and those responsible for critical information systems operations rely on scientific proof (auditable proof) of the performance of IT devices and systems. Physical security systems stakeholders have the same right to get proof of performance like what the organization gets for its IT systems. Qualitative opinions and guesswork from vendors, security staff or integrator service technicians are not sufficient.

It is long past time to elevate security systems management to a level of practice that is appropriate for today's 21st century information-technology-based security systems. *IT has already proven the cost and system uptime benefits.* Businesses expect, and most mandate, that their significant technology investments be properly managed and well-performing.

It is time to start making the business case for IT-class systems management of physical security systems.

About Ray Bernard

Ray Bernard, PSP, CHS-III is the principal consultant for Ray Bernard Consulting Services (RBCS), a firm that provides security consulting services for public and private facilities. For more information about Ray Bernard and RBCS go to www.go-rbcs.com or call 949-831-6788. Ray is also an active member of the ASIS Physical Security Council and IT Security Council. Follow Ray on Twitter: @RayBernardRBCS. These article excerpts are copyright © 2016 by RBCS.

About Viakoo

Viakoo is operational intelligence for physical security systems. Leveraging purpose-built technology Viakoo quickly and automatically detects physical security system failures, diagnoses the problem, then alerts users and tells them how to fix it. With Viakoo users:

- improve reliability and performance
- gain critical insight into physical security systems
- capture valuable operational performance information
- eliminate lapses in security coverage

Operational Intelligence (OI) is a category of real-time dynamic business analytics that deliver visibility and insight into data, streaming events and business operations. Viakoo Inc. is an Industrial Internet of Things (IoT) company, located in Mountain View, California, USA.

Viakoo, Inc.
1100 La Avenida St, Building B
Mountain View, 94043

www.viakoo.com
(855) 858-3400
info@viakoo.com