EBOOK

5 BLIND SPOTS OF PHYSICAL SECURITY

How to Find and Mitigate Your Hidden Risks

RECONASENSE

TABLE OF CONTENTS

DETECTING UNSEEN THREATS

Detecting potential physical security threats is much like driving a car: just when you think you see everything, a potential risk pops up out of nowhere, unseen, from one of your blind spots.

Fortunately, innovative smart technology eliminates blind spots by using sensors that detect risks to make driving safer. As a result, cars are now "intelligent." So why are physical security tools lacking similar intelligence?

Today's security infrastructures are undergoing a digital transformation in response to this ever-changing dynamic environment. As the world continues to shrink, almost everything is interconnected, making people and organizations more vulnerable to threats, both internal and external.

As this emerging security intelligence and technology generates new data—from access control records, video, IoT devices and sensors—security teams need new ways to reduce unseen security risks.

By leveraging an integrated, risk-aware security system, organizations see how a unified platform illuminates and detects security blind spots for improved life safety, minimized risk and increased operational efficiency.

BLIND SPOT #1
LEGACY ACCESS CONTROL SYSTEMS

"You can't control what you can't measure"—it's a tried and true management best practice, especially true for security platforms.

Unfortunately, traditional Physical Access Control Systems (PACS) have not listened. Legacy PACS have a limited capacity to generate meaningful statistics that measure access activity. That means security teams are blind to increasing threat levels or risks, as they lack an effective means to adjust permissions when risk is present.

For example, traditional PACS categorize individuals into simple groups, treating them as if they are all the same. However, humans know that no two people are alike: each of us follows unique behavior patterns and routines on a daily basis.

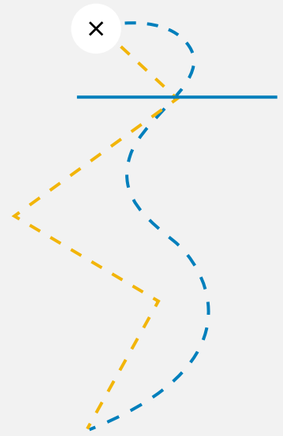
Conventional PACS fail to detect behavioral abnormalities in real-time as they use technology based on older static access controls without analytics. They simply cannot evaluate what is on the other side of the door and thus fail to sense potential dangers before granting that 'individual' permission to access a location.

ROLE-BASED CATEGORIES MISS INDIVIDUAL BEHAVIORS

Most often, organizations structure their physical access permissions around groups based on their role in the organization. Traditionally, these systems see the group but not the individual, incapable of looking beyond that category for other out of the ordinary pieces of information.

Discover abnormal access activity — with or without PACS during an unusual situation and recognize high-risk activity that may not show up as an official policy breach. By analyzing new data to assess activity as being within the parameters of normal or as they become abnormal behavior, and then report to the security team to take action if appropriate.

Case in Point: Routine Deviations



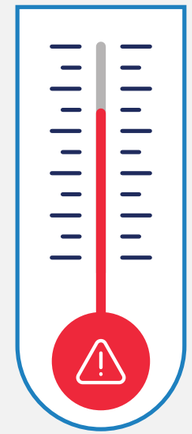
A new employee establishes habits, figuring out by trial and error what's the best route to get across campus. A few months into the job, an unusual circumstance intervenes—perhaps a parent needs care, or the car breaks down—and their access habits change. Traditional access control systems cannot detect these deviations in individual habits. They fail to see the individual, as they cannot look beyond an assigned role or category. An intelligent access control system that is risk-aware would be able to identify a change in behavior and flag security teams for inspection or remediation.

ONE-WAY SYSTEMS CAN'T LOOK AT THE OTHER SIDE OF THE DOOR

Sometimes, threat exists inside the building, and can put individuals in the path of danger. A legacy access control system checks only for authorized permission to grant access for an individual, regardless of whatever potential hazard is present on the other side of that access point. Legacy systems are unable to detect if the environment poses a risk to the user.

PACS that integrate with other systems, e.g., building automation systems, can detect abnormalities based on a variety of environmental factors—a change in radiation levels, temperature, lighting or humidity—which is then factored into consideration in real-time before granting permission to any individual.

Case in Point: Safety First



Many facilities house hazards of various types: radiological, chemical or even biological. These conditions can create hazards where the internal room temperature is too hot for a human to enter safely. Traditional access control systems are not able to detect these issues in real time, and could essentially allow access to what could be a life-threatening situation. With an intelligent, risk-adaptive access control system, the user would be temporarily denied permission if those environmental risks were present.

BLIND SPOT #2
SEPARATE SILOS OF DATA

With the increased amount of data available along with the growing number of connected devices and facilities to manage, simply adding more surveillance and forensic capabilities will neither effectively minimize risk, nor will it help security teams take the right action in the midst of an emergency. **However, an interoperable approach that is risk-based and contextually aware pulls together all the relevant data and translates it into a common language.** Security teams can then make sense of the data quickly and easily to identify and prioritize activities in areas of higher risk.

When data silos exist—especially multiple systems speaking different languages simultaneously—the inevitable outcome is noise. **Attempting to hear everything while only listening to what is most important is virtually impossible for the average person.**

Case in Point: Noise-Cancelling Security

Consider the sensory overload at an airport. Just like a busy Security Operation Center (SOC), airline terminals are noisy environments. Fortunately, innovators have developed noise-cancelling headphones to filter out extraneous noise so people can listen only to what they desire. With an intelligent and integrated platform, SOCs have a similar tool that listens to everything, filtering out noise and allowing operators to focus only on the most relevant risks at the time.

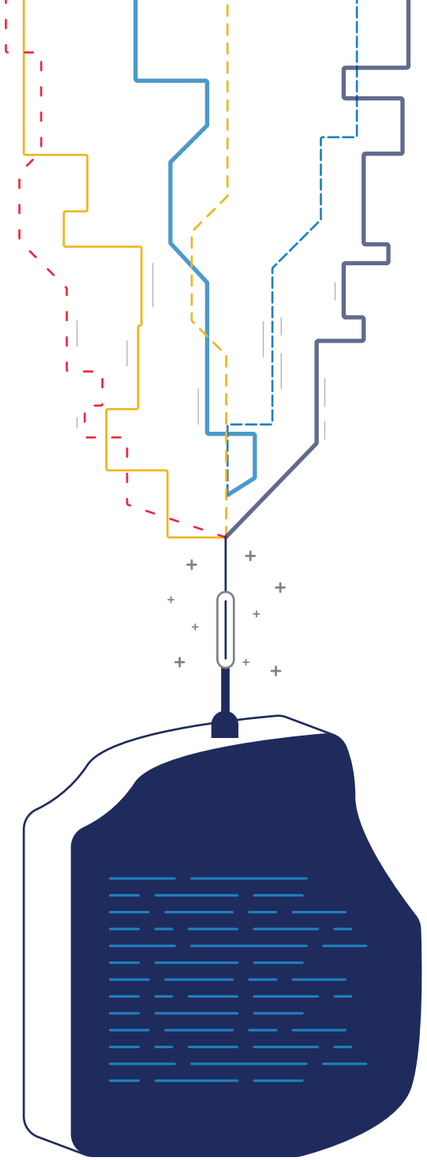
Or consider this: Imagine attending a United Nations (UN) conference to unravel the world's problems. Everyone in the room wears headphones to hear translations in real time, enabling them actively to contribute to the resolution. Suddenly, the leader breaks in announcing an asteroid is hurtling towards the earth. Just as suddenly, the translation system shuts down. What was once a unified discussion becomes dozens of disparate languages all colliding in confusion, with each person contributing to the noise in their own language or "silo."

While noise is not the norm at the UN, this case in point scenario is very much like busy SOC environments. Operators invoke a ‘swivel neck’ to translate multiple disparate inputs into actionable commands and determine if the incident is a risk or not. This frenetic activity contributes to alert fatigue. Operators become overwhelmed by a combination of nuisance and false alarms, desensitized to real threats indistinguishable from true early warning signals.

These “unified” platforms are not so unified. Rather than translating inputs at the data base layer into a common language, they project multiple interfaces onto a common screen. Although these traditional systems may be sharing a common view in a presentation layer, the individual systems are still not communicating with each other.

Traditional platforms are not a true system of systems: they rely on humans to make interpretations of data in real time. Unfortunately, operators are left with the burden of reading multiple languages simultaneously, trying to digest 10 windows of information simultaneously. This is a difficult, if not impossible task to accomplish.

To prevent data blind spots, a true unification platform translates all these different languages into a single, common language. Think of it as a Rosetta Stone for physical security. By normalizing streams at the database layer, the unified platform centralizes all sensor data and formats it into one common log. Both operators and machines can now easily understand potential threats across the entire operation system, drastically reducing nuisance and false alarms.



BLIND SPOT #3
LIMITED ACCESS TO BIG DATA

Risk hides everywhere. Traditional physical security systems rely on only the inputs from their internal systems. This can lead to omission of external forces that could impact security postures.

To develop a truly proactive, real-time security system, the platform needs as much information as possible to see virtually everything across all possible systems. Most importantly, security systems must exceed traditional inputs and incorporate information from non-traditional data sources into security analysis profiles.

Consider social media and the Internet: two non-traditional big data streams that can help expose many potential threats.

SOCIAL MEDIA

The advent of Facebook, Twitter, LinkedIn, Instagram, and more has created its own torrent of data streams. However, the ability to harness that information can provide new insight into potential security blind spots.

Case in Point: Tweets Prepare for a Protest

A company tracked Twitter hashtags and geo-locations of an impending demonstration nearby that would cause possible disruptions in their facility operations. With social media integration, the operation was able to respond eight minutes faster than police could intervene. Thus the company adjusted access control permissions and reallocated guard resources to prevent the incident from becoming a true threat to safety and security.

INTERNET

Tracking ubiquitous data across multiple sources can help predict potential impacts to operations and the safety not just of goods, but human life as well. For example, security intelligence can leverage weather systems, news feeds, live streams, etc., to assess how workers and assets could be affected while in transit from one location to another. With the right level of insights, providing alternative routes and communications can be more effective in keeping everyone safe.

Case in Point: Risky Weather Patterns

One transportation company needed to send trucks loaded with hazardous materials across the country in the dead of winter. Beyond analyzing for any potential terrorist threat levels, the company pulled in weather channel data across key roadways. By seeing which roads were blocked due to extreme weather conditions, and sighting any potential hot spots of known potential subversive risks, the company was able to predict the best route and avoid potential danger.

BLIND SPOT #4
REACTIVE SECURITY POSTURE

Security experts understand the importance of getting ahead of the threats rather than relying on forensics and alerts after an event has occurred. Finding guards who can intake all the information from the various SOC systems and predict a threat is a nearly impossible and unreasonable expectation. Most humans lack the analytic capacity of data scientists. In fact, many risk-expert's analyses can be limited to basic Boolean search, breaking down logic into simple "if then/then this" logic streams. Is this a breach? Or not? If so, then what?

Case in Point: Proactive Security IS Rocket Science

When NASA was plotting the re-entry of spacecraft into the atmosphere, they began to understand the enormity of data needed in real-time analysis. The ship would be prone to 20 forces of inertia, axis of motion, pressures, speed, acceleration, etc., the list goes on. The astronauts could not provide auto-adjustments to all the systems required for safe re-entry. Communications to Houston took too long to help in real-time. So instead, they designed an neural network to analyze the data and provide corrective measures in real-time. This same technology is now available to help predict threats and mitigate security risks.

TWO STEPS TO A PROACTIVE POSTURE

1

Remove Computer Logic Restraint

Security systems are traditionally embedded in basic computer logic. They lack the ability to look at the thresholds dynamically, bound by simple-logic programming. Further, they are reliant upon humans to interpret the data. **With so much data blinding operators every second, legacy systems fail to provide proactive interventions in real time or see threats coming.** They only report what has already occurred.

2

Remove Human Constraints on Logic

Most people cannot remember what they had for lunch last week or the color of a co-worker's shirt from yesterday. Humans process an enormous amount of data daily, which can cause distractions. External factors such as fatigue or illness also come into play. People can only do one thing at one time. Even when knowing what to look for, humans can miss critical inputs due to any or all of these factors. We are simply incapable of catching everything, everywhere, all of the time.

That's where an enhanced security system comes in. Driven by refined logic to detect and analyze vast data streams from multiple inputs, the system determines what are normal deviations before they become breaches. These intelligent systems can look at complex events, detect diverse thresholds and provide real-time notification or post-event reports. Most importantly, they supplement the human logic stream—never removing it—in order to augment data feeds so that operators have a chance to see potential threats proactively, instead of reacting to an existing incident.

BLIND SPOT #5
IGNORING THE HUMAN ASPECT

Obviously, trying to see all these blind spots is meaningless without the human touch. Machines may be adept at processing endless data points quickly but humans are far more capable of deeper analysis and cognitive reasoning, which leads to making the most informed decisions.

A VISION FOR ENHANCED PHYSICAL SECURITY

Enhanced platforms have become the new benchmark for physical security systems. With a combination of intelligent insights and a truly unified data into a common language, ReconaSense will become the industry's standard for providing a risk-adaptive physical security and access control solution.

ReconaSense delivers the only enhanced, proactive security platform by seamlessly unifying security, sensor and IoT device and other system data that can "see around the corner" to recognize potential threats and mitigate risk.

See how ReconaSense shines a light on these types of threats and others you may not see.

REQUEST A DEMO

ABOUT **RECONASENSE**

ReconaSense helps protect people, assets, buildings and cities with its next-gen access control and converged physical security intelligence platform. ReconaSense identifies and mitigates potential threats and attacks before they happen, giving security teams the ability to go beyond managing data and individual alerts to achieving true situational awareness and rapid response capabilities.

LEARN MORE AT **WWW.RECONASENSE.COM**

+1 512.220.2010
insider@reconasense.com

RECONASENSE