# Let's Get Physical: The Emergence of the Physical Threat

A Spire Research Report – June 2003

By Pete Lindstrom, Research Director

Spire Security, LLC
P.O. Box 152, Malvern, PA 19355
www.spiresecurity.com

# Executive Summary

Sometimes we spend so much time worrying about cyber-attacks that we forget about the basic problem of physical threats. There are many types of physical threats that must be factored into a security program, including theft, sabotage, human error, and environmental disruption.

When implementing a physical threat monitoring system, an enterprise must deploy sensors in sensitive areas and along likely attack paths, capture all available information that can help identify the specific problem, and develop a system that can aggregate this information and distill it into salient details that must be acted upon.

This white paper defines a number of physical threat types and discusses the objectives of physical threat monitoring. It then discusses the NetBotz® solution within the scope of physical threat monitoring and explains the NetBotz approach to providing a solution for physical threat monitoring.


## About Spire Security

Spire Security, LLC conducts market research and analysis of information security issues and requirements. Spire provides clarity and practical security advice based on its "Four Disciplines of Security Management," an operational security model that encompasses identity management, trust management, threat management, and vulnerability management. Spire's objective is to help define and refine enterprise security strategies by determining the best way to deploy policies, people, process, and platforms in support of an enterprise security management solution.

This white paper is sponsored by NetBotz. Spire Security maintains its independence regarding the content and assertions that is the product of years of security audit, design, and consulting work.

# The Emergence of the Physical Threat

## Table of Contents

The Intersection of Technology and the Physical Threat . 1
- Overview ........ 1
- Physical attacks against systems ........ 2
- Physical attacks detected by systems ........ 2

Physical Threat Types ........ 2
- Theft (physical and virtual) ........ 2
- Sabotage ........ 3
- Human error ........ 3
- Environmental disruption ........ 3

Objectives of Physical Threat Monitoring ........ 3
- Monitor all environmental factors ........ 3
- Deploy sensors where needed ........ 4
- Comprehensive protection ........ 4
- Physical resilience ........ 4
- Analytical capabilities ........ 4

The NetBotz solution ........ 4
- Secure ........ 5
- Solid State ........ 5
- IP Connectivity ........ 5
- Multi-sensor collectors ........ 5
- Intelligent analysis software ........ 5
- SNMP Aggregator ........ 5

Spire ViewPoint ........ 5

# Introduction

Long before there was anything called "cyberterrorism" there was terrorism. Before there were software bugs, there were bugs getting caught in computers. Long before there were software errors, there was human error. The virtual world is not safe, but the physical world has the right of first refusal on risk, if only for the more drastic downsides.

Computers and networks are taking over enterprises, becoming ubiquitous as they infiltrate our primary business processes to the point where these systems are crucial to the success of the organization. This growth in physical infrastructure as well as its growing significance to an organization has created the need to protect the systems themselves, not only from cyberattacks, but from the physical attacks that can be perpetrated against them.

A number of parties play a role in physical threat monitoring. Security departments have played a traditional role in protecting all of the assets in an enterprise. The Facilities group ensures that the physical plant runs smoothly and reacts to environmental concerns. Information security professionals protect the data and system usage that is increasing in value. Each of these constituencies has a stake in the success of any protection plan. How they work together and leverage technology to protect technology is the topic for the rest of this paper.

# The Intersection of Technology and the Physical Threat

## Overview

As we build smarter software, we increase its value. The need to protect the software application and its data is obvious, but there is another side effect of smarter software: it can be put to use in the protection itself. IP- based physical threat monitoring systems can leverage the same infrastructure they are protecting.

Information security professionals have long focused on virtual risks, but at some point all things virtual become physical. It is that crossing point--where physical infrastructure and systems provide an access point to the virtual world -- that the link between physical threats and virtual threats is most apparent.

Two perspectives exist that highlight the need and power of new physical threat monitoring systems – protecting systems from physical attacks and using systems to make protection more effective.

### Physical attacks against systems

Sometimes, the most apparent attack paths get ignored in favor of what is "in vogue." In a lot of ways, that is what is happening in the information security world. Certainly, cyberattacks and hackers and worms are very real threats. But we can't ignore those attacks that are targeted against physical computing infrastructure and so must factor in other threats to these assets.

One example of this kind of threat is apparent with today's multinational corporations. Information security professionals may disregard the threat of physical attacks when attempting to thwart the hack attack coming from the other side of the world, but entities with facilities in countries with diverse geopolitical ideas may have a serious physical threat from employees who can tap networks or steal hard drives.

### Physical attacks detected by systems

The power of software is in its ability to consistently process large amounts of data and identify nuggets of information in an efficient and effective manner. The challenge of physical threat monitoring is always in identifying an attack before it occurs, or determining the likelihood of a problem in advance. Applying the power of software creates an opportunity to more effectively protect an enterprise.

For example, the failure of a network hub may be identified because it stops sending its status reports. A *virtua*l monitoring system can identify that something is wrong. A *physical* threat monitoring system that has links to the software can do more. It can identify the same problem and then provide information about the cause of that failure--temperature, air flow, or water existence in the physical facility, for example. The decisive benefit comes from the existence of a secure camera in the room that can send images back through the wires to an operations console. In this way, the full picture of what is happening can be created and the problem solved more quickly.

Building the story around a threat first involves understanding the variety and types of physical threats that exist today.

# Physical Threat Types

Everyone has a different mental picture of a "physical threat." Often, the picture that forms first does not provide the clearest, broadest perspective on threats that exist. When it comes to networking infrastructure and equipment, there are a number of threat types that must be considered when evaluating the physical threat. They are discussed here.

### Theft (physical and virtual)

Theft is the most obvious threat, particularly for those individuals with a security background. At the intersection between physical and logical worlds, theft can occur in either place. Computing and network equipment has long been stolen and resold on the black market, simply for the value of its computing power. In addition, physical attacks against logical security can be easily perpetrated. Logical attacks can occur at system consoles, through available ethernet ports, and in network equipment rooms (wiring closets).

### Sabotage

A close cousin to theft, the deliberate destruction of equipment is an oft-used technique for "teaching lessons." Anyone with a grudge against an organization may provide some risk of sabotage against sensitive systems. Nowadays, terrorists are often considered when evaluating the likelihood of physical sabotage to mechanical and computing equipment.

### Human error

A much more common occurrence, though often not considered a "threat," is human error. Stories abound of the "early days" of computers when janitorial staffs would unplug mainframes to sweep behind them, and then plug them back in when things were clean. While incidents like this are highly unlikely to occur in today's data centers, ubiquitous networks have led to pieces of the computing infrastructure being placed in precarious places. It is not difficult to imagine human error resulting in equipment being jostled out of place (say, in a copy room or janitor's closet) and unplugged, reset by mistake, or knocked off a shelf.

### Environmental disruption

Perhaps the most prevalent threat today is simply the "Act of God" and related manmade environmental problems. Fire tears through buildings. Floods caused by plumbing or natural means destroy infrastructure assets and data. Electricity spikes and power outages caused by thunderstorms can wreak havoc on computing equipment, particularly when backup generators aren't regularly tested. These threats are common in any organization today.

All of these threats must be evaluated against the likely risks in the environment. There are basic objectives for building out a strategy for physical threat monitoring.

# Objectives of Physical Threat Monitoring

One thing is certain with physical threats – they exist everywhere, in various magnitudes and risk levels. When monitoring for these threats, it is important to keep in mind some basic objectives:

### Monitor all environmental factors

Humans deploy all of their senses when detecting threats. Monitoring systems should follow the same approach. Sensing heat, alarms, gases, pressure and movement, for example, are key attributes of the sensors being deployed. One of the key senses is sight, and cameras are a key sensor to ensure that visual access to remote sites is available. A physical threat monitoring system must support a wide variety of sensor types to develop a complete picture and understanding of a given situation.

### Deploy sensors where needed

The obvious first step in physical threat monitoring involves evaluating those areas that are susceptible to attack. Data centers, wiring closets, and areas where guards or other physical access control are weakest—for example, remote distributed locations--round out those areas that deserve attention. The key is in sensor deployment. When monitoring for physical threat, sensors must be portable and flexible enough to be deployed anywhere they are needed. Sensors are ineffective if they have no way of collecting data and storing it in some way for future analysis.

### Comprehensive protection

Deploying sensors only in areas deemed “sensitive” creates a paradox for the intruder. Rather than focusing on items of greatest value, or areas of biggest risk, the tables are turned so that the intruder then seeks out gaps in any defensive strategy. Deploying sensors along likely avenues of approach, then, becomes the logical second step to protecting sensitive areas in any deployment strategy.

### Physical resilience

Any physical threat monitoring system must be able to withstand physical attack itself. Sensors require protection against damage from attackers, environmental activity, and routine negligence. The goal is to deploy sensors that need little or no intervention over extended time periods – they just work.

### Analytical capabilities

It is clear that multiple types of sensors add value by providing individual clues to the threat status of the infrastructure being monitored. As more data is being aggregated from multiple sensors, however, the value is lost if the back-end software does not provide strong intelligence. Physical threat monitoring solutions need the ability to filter, correlate, and otherwise evaluate the data to determine a course of action.

# The NetBotz solution

NetBotz was formed in 1999 to leverage new technology to protect enterprises from the physical threat against its network and computing equipment. The attributes of its physical threat monitoring solution include:

### Secure

The architecture of the NetBotz solution provides security of transmission by encrypting communications to protect against data being captured or inserted into the information stream. In addition, the sensors can be deployed in a protective casing that is tamper resistant. Finally, the ability to deploy and manage multiple sensors provides redundancy to protect against a focused attack on the sensor.

### Solid State

There are no moving parts on NetBotz sensors. Moving parts are susceptible to physical and mechanical damage that require site visits to repair. By developing the digital capabilities of the system, NetBotz was able to eliminate the need for mechanical features and reduce the likelihood of failure.

### IP Connectivity

Existing monitoring systems require separate physical cabling for CCTV functions. NetBotz uses the same technology it protects by integrating into the typical IP network. This allows sensors to be deployed anywhere the network is to protect its components. In addition, it eliminates the need for duplicate cabling using different wire types.

### Multi-sensor collectors

In keeping with the "human senses" model of threat monitoring, NetBotz provides the ability to collect data from multiple sensors in order to aggregate information into a single place.

### Intelligent analysis software

The more intelligent the software, the quicker individuals can respond to threats. As technology creates the ability to aggregate data from many places, it creates a level of analysis complexity that is best resolved through analytical software. In the end, this creates an efficient and effective approach to the specific needs of identifying and reacting to attacks.

### SNMP Aggregator

Part of the capabilities associated with a physical threat monitoring system that works with the IP network is its ability to also collect SNMP data and pass along the data at appropriate times.

## Spire ViewPoint

Protecting information systems from the physical threat can easily fall into a no-man's land. Information security professionals are distracted by worms and viruses, physical security guards monitor the entrances and exits to buildings, and facilities personnel are spread thin trying to keep the entire site up and running. When it comes to protecting the physical infrastructure of the computing environment, each of these constituencies may have overlapping responsibilities that are unclear and result in some physical threat monitoring left undone by the assumption that another group is addressing the problem.

Physical threats have a significant impact on information systems – that is apparent the first time the lights flicker in a thunderstorm, and more apparent when a server turns up missing. A strong physical threat monitoring solution is crucial to the ability to maintain the computing facilities, including wiring closets and remote data centers, and ensure continuous, secure computing.

The NetBotz physical threat monitoring solution is designed to address threats against the computing infrastructure and leverage that same infrastructure to gain the benefits of a digital world. The added capabilities, when leveraged against physical threats, can provide a much more efficient and effective monitoring solution than the existing analog infrastructure.

## Contact Spire Security

To comment about this white paper or contact Spire Security, LLC about other security topics, please visit our website at www.spiresecurity.com.

This white paper is sponsored by NetBotz. Spire Security maintains its independence regarding the content and assertions that is the product of years of security audit, design, and consulting work.