INTERNATIONAL FOUNDATION FOR PROTECTION OFFICERS
Knowledge to Protect

Submitted: Kevin Coleman **At:** cyclesandi@earthlink.net

Title: The Intersection of Physical and Cyber Security **Date:** Feb 24, 2016

The role of private security forces is dramatically changing. Analysis has concluded that the role and responsibilities of private security will continuously change and the pace of change is about to increase sharply. Today, private security forces are essential to ensuring the security and safety of persons and property, as well as intellectual property (IP) and sensitive corporate information (SCI). All that change is being brought about by critical needs that are being driven by the current threat environment. Today, private security forces are responsible for protecting much of every nation 's critical infrastructure systems and public facilities as well as protecting the assets (physical and cyber) of corporate.

The increasing relevance on private security forces to monitor private and commercial properties and their efforts contribute to the country's safety and security requires private security forces be trained on topics focused on the intersection of physical and cyber security. By far, the most common cyber/physical security issue is the physical theft of an organization's information assets (data, hardware and software). I am sure we are all familiar with the term dumpster diving. For anyone not familiar with that term, it refers to someone on the inside throwing something of value away and have someone else retrieve that item when the trash is emptied to the dumpster outside. Here are a few other common cyber/physical attacks that all physical security professionals must be on the lookout in order to detect them.

Direct Physical and Cyber Intersections

1. Cyber/Physical Attack involves placing one or more malicious software (malware) infected USB/Thumb Drives somewhere on the exterior of a facility. A well-meaning employee or contractor finds the device and plugs it into a corporate computer. Once inserted the malware infects the organization's computer, and in many cases spreads across the wireless or wired network. In one case, a visitor found the USB/Thumb Drive and turned it in to the security guard at the main entrance. The guard then plugged it into the computer to try and identify the owner. Once the guard did that, the malware spread throughout the organization.

2. Cyber/Physical Network Sniffing involves an occupied or unoccupied vehicle parking near the facility with a network sniffer operating inside the vehicle. The network sniffer records ALL wireless network traffic. Once the vehicle/sniffer is retrieved, all that unencrypted traffic that contains personal information, login information, proprietary information and even competitive strategy information that flowed across the wireless corporate network is accessed. It can be used for competitive advantage, sold to competitors, or in some cases held for ransom.

Indirect Physical and Cyber Intersections

1. Cyber/Physical Bullying involves aggressive behavior typically emotional abuse directed toward a specific target. It is a distinctive pattern of deliberately hurting, harming and humiliating a specific target. This behavior can either be overt/direct, using physical activities such as fighting, hitting or name calling. It can also be covert and indirect, using techniques such as gossiping in the real world or online, social media, text messaging or leaving someone out on purpose. You should not think for a moment that cyber/physical bullying doesn't occur in the workplace!

2. Cyber/Physical Mobbing involves a group of people which is formed to "ganging up" on a target. Targets commonly include individuals, co-workers, subordinates or superiors, and this is done to influence or force someone out through malicious activities including discrediting, humiliation, embarrassment, innuendo, intimidation, isolation or purely through rumors. Some referred to Cyber/Physical Mobbing as general harassment such as commonly done at school, in public, at shopping malls or even in the workplace.

These are just a few of the hybrid cyber/physical security threats that exist. There are others. For example, tools are available to intercept files being sent via wireless to printers. Thinks of all the data that gets printed. One study determined that the average U.S. office worker prints 10,000 pages per year. That is a huge amount of data.

There is one more cyber/physical security risk that needs to be presented here. Did you ever think of drones as a hybrid cyber/physical security risk? Well, it turns out they actually are! Recently while at a business office complex a drone with a camera was hovering just outside a meeting room window on the executive floor! On the wall opposite the windows was a whiteboard filled with pricing information and the organization's business sales strategy.

The total number of hybrid threats are about to increase substantially. The Internet of Things (IoT) has been estimated to top 21 billion individual devices by 2020. That is a significant increase in the cyber perimeter that must be defended. Most of those devices will be directly connected to the Internet without have basic security protection (no firewalls or anti-virus defenses). IoT technology does not stop there. Recently I saw a pair of shoes that had sensors built into their insoles. The sensors tracked the number of steps, continuous location information, and time stamped the travel and locations. That would allow organizations to much more closely monitor the location and activities of private security forces for accountability and the safety of individual. We have just scratched the surface when it comes to examining the intersection of physical and cyber security. There is so much more to this issue.

INTERNATIONAL FOUNDATION FOR PROTECTION OFFICERS

Knowledge to Protect

Everyone involved in physical security needs to understand the basics of cyber security as well as the common cyberattack techniques that intersect with the physical world. Like it or not, this is the new reality of the profession. The global demand for private security services is expected to grow by 7.4 percent through the end of 2016. That means it will soon top $400 billion USD. Interestingly enough the global annual cost of cybercrime is now estimated at exceeding $400 billion USD. Many of the physical aspects of cyber security are falling to traditional private security resources. Are your prepared? If you aren't, that could cost you the next job. The time has come for every private security resource to become trained on all of the physical aspects of cyber security and start contribute to reducing this growing risk.