



Cell Phone Threat Mitigation Tactics

Practical Considerations from the Frontline



www.airpatrolcorp.com

Introduction

Cellular phones have come a long way since their introduction in 1973. Improved network speeds and more powerful features have combined to transform handsets into devices that have more in common with a computer than a traditional telephone. Today's cell phones have amazing processing capabilities, on board and removable memory, email clients, text messaging, cameras—and employees as well as criminals recognize their benefits as powerful tools.

The consequence of having these new hybrid cell phones in the hands of hundreds of millions of people has huge security and regulatory implications for many industries. Terrorists, spies, insider traders, prison inmates, identity thieves, and other criminals are using cell phones as a tool to launch insidious attacks, execute illegal activities or compromise classified information.

In government agencies, prisons, research laboratories, financial trading floors and other environments, where policy enforcement and compliance with data security regulations are mission critical, the requirement for effective cell phone detection and location technologies is becoming essential. Wireless Threat Management Solutions with cellular location capabilities can be used to effectively enforce bans on cell phones or monitor their usage—helping to turn the tables on would-be criminals by providing a highly reliable and sophisticated solution for detecting, and more importantly, locating the devices they rely on to perpetrate their crimes.

This white paper identifies the common security challenges introduced by the growing popularity of hybrid cell phones. By discussing the necessary components of a comprehensive cell phone policy enforcement plan, this paper details the immediate actions security managers should take to formulate a cell phone threat

mitigation strategy that will protect proprietary assets and help maintain compliance with industry regulatory requirements. In addition, this paper provides an overview of the issues a security manager should consider when evaluating and choosing a cell phone detection solution.

Productivity Super Hero, IT Security Achilles Heel

Cell phones organize our lives, keep us connected and informed and provide us with hours of entertainment—music, videos, games, and more. According to one wireless industry group, there are more than 250 million wireless subscribers in the United States. The growing popularity of hybrid cell phones raises new issues for employers, government agencies, research institutions and other organizations around the globe. Cell phones with built-in camera or data storage and transfer capabilities are being used to facilitate the theft of sensitive information, compromise privacy rights or conduct other illicit activities.

Cell phones with cameras threaten security more than traditional cameras because they are smaller and more easily concealed. A picture can be taken while a user appears to be making a phone call or sending a text message. By the time it is noticed that photos have been taken, the images might have been sent to others or even posted on the Internet. Text messaging, or texting, is especially problematic because text messages, unlike e-mails, do not show up on company servers. By default, they are invisible to the company, so the people sending them could be saying anything, from sharing proprietary information to ordering illegal trades from the financial floor.

Invasion of Privacy

News networks have uncovered camera phones being used to watch unsuspecting individuals in gyms, department store

dressing rooms, locker rooms, and tanning salons. In health care, the concern spans beyond a privacy issue to a legal obligation to maintain patient confidentiality in compliance with Health Insurance Portability And Accountability Act (HIPAA) guidelines. In addition, camera phones pose a problem in courthouses where photographs can compromise the identity of undercover police officers testifying.

Espionage

There are a growing number of instances in which an employee or visitor in a government agency, corporate facility, factory, research and development lab, or business exposition has photographed sensitive information using a cell phone camera and sent the data instantly elsewhere. Agencies and businesses like General Motors, Intel, and Lockheed Martin are prohibiting the use of camera phones—afraid of James Bond-style espionage, in which employees take photos of confidential documents and sell them to third parties. In addition, cell phones can be used as remote eavesdropping devices to intercept highly sensitive conversations that occur in the boardrooms of corporations and legal firms, and in classified areas such as embassies, and government agencies and contractors.

IT Policy Circumvention

Mobile phones may be used to elude security policies, such as call recording requirements. Reports point to the illicit use of a cell phone—used to circumvent monitored phones lines—as the main cause of the recent Société Générale breach, which cost the bank almost \$7 billion in losses. The use of contraband cell phones within prisons is one of the biggest problems facing corrections institutions. Using a cell phone, inmates can avoid monitored phone lines to continue their criminal activities from inside, plan escapes or contact victims on the outside.

Equipment Interference

Beyond security breaches, cell phones can interfere with the proper functioning of equipment in hospitals, airplanes and other highly sensitive environments. When a cell phone is turned on, it transmits up to 3 watts of power. If the cell phone creates interference that overlaps with radio frequencies in use by equipment, then messages between people may be garbled or faulty messages may be sent between pieces of equipment. The interference can potentially continue as long as the cell phone is turned on because the cell phone and tower handshake with each other every couple of minutes, which results in a burst of data during each handshake.

Detonation of Bombs and Explosives

Terrorists have long used cellular phones to trigger improvised explosive devices (IEDs) in their attacks on civilians and military personnel throughout the world. Cell phones are arguably the most ideal device to trigger Weapons of Mass Destruction (WMDs). Cell phones are convenient for terrorists because they are very common, easily concealed, and can be called from anywhere in the world. With enough battery power to detonate a bomb, automatically synchronized and addressable cell phones provide terrorists with an advance level of precision and control when targeting airplanes and other large public areas such as airports, sports arenas, public buildings and gathering places.

Threat Mitigation Strategies

As technologies and threats evolve, so must corporate security policies and practices. In today's high-tech and interconnected world, every corporation needs a well thought out security strategy that addresses cell phone vulnerabilities in addition to more traditional threats.

The Business Challenge

Many people believe it is their inalienable right to have a cell phone on and ready to be answered at all times – regardless of whether they are at work, in public or on the go. But as cell phone capabilities continue

Reports point to the illicit use of a cell phone—used to circumvent monitored phones lines—as the main cause of the recent Société Générale breach, which cost the bank almost \$7 billion in losses.

to evolve, it's becoming increasingly important for today's employers, institutions and agencies to evaluate the threats posed by the infiltration of these devices and then formulate their risk mitigation strategies accordingly. Often organizations will need to balance the trade offs between security and productivity as security solutions inject “speed bumps” in the paths employees use to access and exchange data.

Policies: The First Line of Defense

Organizations need policies, standards and procedures to enforce information security in a structured way. Enterprises are slowly responding to real and potential misuse of cell phones. Just over half of members surveyed by the Society for Human Resources Management have written policies addressing the use of standard cell phones. Fewer have written policies for the use of camera phones.

Conducting a thorough risk analysis, which includes a comprehensive security vulnerability assessment, can help organizations determine areas of risks. The assessment results, combined with a proper policy framework and standards, should determine which policies are necessary. For

example, while it may be sufficient for some organizations to prohibit employees from photographing important business assets, such as documents or equipment, other organizations such as research institutions and classified government agencies may find it necessary to ban camera cell phones completely from the premises. As a further precaution, organizations can consider putting sensitive items or data in special areas that have increased security and provide better training or guidelines to employees to watch for behavior involving camera phones that may inappropriate.

Camera phone bans are increasing in popularity. There are many public and government locations where camera phones are banned or even confiscated. The first to ban them were federal courthouses. *Daimler Chrysler* has added to its security policy a ban on camera phones, and *Texas Instruments* has a written company policy prohibiting all types of recording devices on the premises, including camera phones.

In reality these bans and prohibitions may be difficult to enforce. Establishing policies without a means of enforcement is not sufficient to fulfill security directives and protect mission-critical operations. To effectively enforce policies and prevent exposures, organizations need visibility into their operations with the ability to maintain constant and vigilant security. Today's next-generation wireless Threat Management Solutions with cellular location capabilities are providing organizations with the tools they need to reliably enforce bans on cell phones and monitor their usage in restricted environments.

Cell Phone Detection and Location Solutions

Cell phone detection and location solutions identify and alert security personnel when unauthorized cell phones and communications are detected within a monitored area. Using a network of cell phone sensors spaced approximately 75 – 100 feet apart, the system is able to determine the phone's location and displays it on the management console.

How It Works:



1. When a cell phone beacons a cellular tower, places/receives a voice call, or sends an SMS message, the sensors within receiving range of the cell phone detect the activity.
2. The sensors transmit the information they receive over the Ethernet LAN to the server.
3. The server analyzes the data and determines the location of the cell phone.
4. The location of the cell phone and other information about the transmission is then displayed on a facility floor plan within the Management Console and is also transmitted to any email-capable device such as a Blackberry or other cell phone.
5. Network administrator or security personnel are able to monitor or resolve any issues in real-time.

In accordance with FCC rules, cell phone detection solutions cannot block voice communications and text messages, but instead detect and locate their source – allowing security personnel to identify and respond to security threats.

Advanced cell phone detection solutions can send alerts in multiple formats to multiple devices to notify security staff when an unauthorized cell phone is detected and provide complete details of the event along with an image depicting the precise location of the offending device. Alarm zones that are configurable to eliminate false positives provide further benefits to deploying organizations.

A Useful Framework for Comparison

The capabilities of cell phone detection technologies vary greatly. When evaluating technologies it can be helpful to use a consistent, structured framework to understand, evaluate and select the most appropriate cell phone detection solution from amongst the selection of alternatives. The framework presented reflects not only AirPatrol's years of experience and market leadership in wireless security technologies, but also the additional structure and detail required

Cell Phone Threat Mitigation Tactics

to make an apples-to-apples, rather than apples-to-oranges, comparison of various cell phone detection technologies.

Table 1. A Consistent, Structured Comparison Framework

Total Cost of Ownership	Acquisition Cost	What are the initial acquisition costs? This includes all additional hardware, software, servers, services, etc. associated with acquiring the cell phone detection solution
	Deployment Cost	What are the costs to deploy the cellular detection solution? This includes the network cabling costs, ease of installation, ease of setup and configuration, calibration requirements, training administrators, etc. Does the solution leverage existing investments in infrastructure or require its own dedicated network?
	Operating Cost	What are the ongoing operating costs? This may include costs for replacement (e.g., broken / outdated) sensors; ongoing management; upgrades, etc. How many resources are required to manage the solution? Are there hidden costs, i.e. re-calibration requirements?
Strategic Fit (Corporate)	Relative Security	How secure is the implementation? Is it adequate for the information being protected? Does it meet regulatory requirements (if any) for the protection of information?
	Scope/Completeness	Is the solution capable of identifying all cell phones, on all bands (GSM, UMTS (3G), CDMA, iDEN, Nextel)? Does the solution support local cell phone standards, which vary internationally? Can the solution track multiple events including when a phone is turned on, call is placed or SMS message is sent? Can the solution also detect wireless devices? Does the solution record the forensic data needed to support criminal prosecution in legal proceedings?
	Reliability/Accuracy	Will the solution provide accurate device location information, i.e. can I actually locate the offending cell phone? Does the solution detect cell phones when they are not being used to make a call? Does the solution detect cell phones being used for text messaging Does the solution provide the tools/intelligence necessary to reliably mitigate threats in a time efficient manner?
Strategic Fit (Systems)	Interoperability/ Back-end Integration	How easy is it to integrate with back-end resources or applications?
	Robustness/Scale	Does the cell phone detection solution scale to the degree required now? Three years from now?
	Future Flexibility	What future options may be available from the selection of this wireless threat management solution (whether you currently intend to use them or not)? What future options might be of interest? Things to consider might include WLAN deployments, wireless VoIP, use of wireless-capable cellular phones, etc.

In this framework, there are three high-level categories, each of which can be broken down slightly further for a total of nine basic attributes. Any cell phone detection technology can be compared—in a consistent manner—using this simple framework to compare and contrast various wireless threat management alternatives.

Total Cost of Ownership

Cost is a critical consideration, but to correctly calculate a total cost of ownership, organizations must consider *all* the elements of cost. The total cost of ownership for cell phone detection solutions can be great if the sensors require a dedicated network connection. This can add an additional \$600-\$800 per sensor in cabling and switch port costs per sensor.

Sensor range has a major impact on the number of sensors that need to be deployed. For example, to adequately cover an area of 160 x 160 feet, 9 sensors are required if the sensor range is approximately 80 feet, whereas over 80 sensors are required if the range of the sensors is approximately 20 feet. Solutions that feature a lower cost per sensor, greater sensor range, the ability to integrate sensor networks into existing hardwired networks, an intelligent approach to threat mitigation, and automatic calibration capabilities can help to bring down the total cost of ownership.

Strategic Fit (Corporate)

When formulating a risk mitigation plan, it is important to address all threats arising out of the proliferation of cell phone and wireless technologies. After conducting a comprehensive assessment of the risks introduced by mobile technologies, organizations must identify which cell phone threat management strategies will allow them to effectively and reliably identify multiple events (including when a cell phone is turned on, call is placed or SMS message is sent) across all cellular bands (GSM, CDMA, etc.). By adding wireless and RF broadband detection to the standard cell phone location capabilities, enterprises can effectively enforce no-wireless policies or control risks by limiting wireless connectivity to designated areas.

Ease of administration and reliable performance can be equally, if not more important than the technology itself. To quickly and accurately manage cell phone threats, security personnel need a simplified way to monitor and remediate security issues. Configurable alarm zones can help to minimize false positives and event alerts that can be sent to cell phones or other email-capable mobile devices can help speed response times. In addition, reliable device location data can help administrators easily determine whether a security event is malicious and mitigate risks on the fly.

Strategic Fit (Systems)

The success of a security method depends on more than just technology—scalability to accommodate growth and interoperability with existing systems and future plans are all important components to a successful implementation. Whether a solution integrates with and compliments security measures already in place can be an important consideration. In addition, choosing wireless threat management solutions that can be expanded to support multiple wireless methodologies (cellular, wireless, RF radio) can provide future flexibility.

Organizations interested in using technologies to enforce a cell phone bans today may want to consider whether the solution can be leveraged as the foundation for a WLAN deployment in the future. Future flexibility is like having an *option*. Options have real value today, not because you use them today but because they represent something that you could take advantage of sometime in the future. Of course, some options are never exercised—but having options definitely gives you a degree of future flexibility. Whether or not there are firm plans to use these additional capabilities, the option to use them exists and provides additional value.

AirPatrol's Cell Phone Detection Solution

AirPatrol's Wireless Locator System (WLS) solution provides the actionable intelligence network administrators need to confidently manage cell phone threats and enforce bans on cell phones. In addition, the solution easily scales to protect and manage wireless networks from wireless originated attacks as well.

Solution Overview

With the ability to detect and accurately locate all cell phones inside buildings to an accuracy of 10 feet or better, AirPatrol's Wireless Locator System (WLS) solution is also the only technology on the market today that is capable of detecting a cell phone before a call is made. The WLS solution utilizes a revolutionary combination wireless / cellular phone sensor that can detect all cell phones that are turned on and is also capable of detecting all SMS messages sent by a cell phone as well as the presence of all wireless devices. This advanced functionality allows security personnel to proactively respond to potential threats before any actual damage is done.

Sensors can be installed using a conventional wired or wireless Ethernet network. The inclusion of two Ethernet interfaces with "Power over Ethernet" (PoE) enables the sensors to share existing network infrastructure and eliminates the requirement to install additional cabling and provision additional switch ports, dramatically reducing the complexity and cost of deployment.

The location of the cell phone or wireless device, and identifying information, is displayed on the WLS console in real-time. If the detected wireless device is registered with the organization, the name of the registered user is also shown. In addition, alerts can be sent in multiple formats to multiple devices to notify security staff when an unauthorized cell phone is detected. Alarm zones are configurable to eliminate false positives. In accordance with FCC rules, the system does not block voice communications and text messages, but instead detects and locates their source – allowing security personnel to identify and respond to security threats accordingly.

Evaluating AirPatrol Products

The following section uses the comparison framework to give an objective assessment of AirPatrol's cell phone detection solution.

Total Cost of Ownership		
<p>AirPatrol greatly simplifies and dramatically lowers the cost-of-deployment of cell phone detection technologies to less than half of the cost of traditional solutions and enables sensor technology to be integrated into existing network infrastructure, rather than being deployed as a parallel network with a discrete overlay security strategy. Once deployed, administrators can manage the environment from a single easy-to-use console that is capable of concurrently displaying all cellular, 802.11 and broadband radio devices.</p>		
Acquisition Cost	Deployment Cost	Operational Cost
<p>Available as software versus appliance</p> <p>Sensors cost below the industry average</p> <p>Superior sensor range provides greater coverage using less sensors than competing solutions</p>	<ul style="list-style-type: none"> ▪ Leverages investments in existing network infrastructure to reduce deployment costs ▪ Cell phone sensors can be piggybacked onto existing network infrastructure without dedicated cabling and switch ports ▪ Sensors include two Ethernet ports on with full pass-through Power Over Ethernet capabilities to integrate into existing hardwired networks without any cabling and switch port costs and enables sensor networks to be deployed by internal staff 	<p>The visual real-time approach to security enables administrators to act quickly and remediate issues without time intensive analytical investigations</p> <p>Automatically adjusts to dynamic wireless environments without manual intervention –eliminating, ongoing recalibration requirements</p> <p>Once deployed, administrators can manage the entire wireless threat environment from a single easy-to-use console that concurrently displays all cellular activity with the capability to add 802.11 and broadband radio monitoring capabilities</p>
Strategic Fit (Corporate)		
<p>AirPatrol's Wireless Threat Management solution represents the most comprehensive portfolio of wireless infrastructure and endpoint security solutions currently available to deliver a unified corporate-wide wireless threat management strategy that completely addresses all of the security issues related to the widespread use of wireless technology (wireless, cellular and broadband radio).</p>		
Relative Security	Scope/Completeness	Reliability/Accuracy
<ul style="list-style-type: none"> ▪ Monitors the airwaves 24 x 7 to provide a live view of cell phone events and location at a single glance ▪ Effectively enables administrators to enforce cell phone bans or limit cell phone use to designated areas ▪ Able to function without decoding any of the data transmitted by the cellular phone, so that it does not infringe the wiretap regulations prevalent in many jurisdictions 	<ul style="list-style-type: none"> ▪ Identifies all cell phones, across all bands including GSM, UMTS (3G), and CDMA ▪ Reliably tracks multiple events including when a phone is turned on, a call is placed or a SMS message is sent ▪ Detects wireless as well as cellular devices <p>Records events in database for use as forensic evidence</p>	<ul style="list-style-type: none"> ▪ Locates all authorized and unauthorized cellular devices with an accuracy of ten feet or better indoors ▪ Provides reliable location data for threat mitigation ▪ Displays device MAC address for unregistered devices or user identifying information for registered cell phones

Strategic Fit (Systems)
<p>AirPatrol delivers the proven capabilities today's businesses require to protect communications, critical information, and IT infrastructure today and in the future.</p>
Future Flexibility
<p>Can be used as a cell phone detection solution and easily scales to protect and manage wireless networks</p> <p>Supports convergence of voice and data</p> <p>Solution is designed to meet future bandwidth requirements without speed degradation -- Future-ready for new 802.11 standards</p>

Summary

The sophistication of cell phone technology has increased dramatically in the last few years. Today's mobile phones have built-in cameras, data storage and transfer capabilities that introduce new fraud opportunities and threaten the security of proprietary and confidential information. Mobile phones can be used to circumvent IT policies, such as call recording requirements, or as a remote eavesdropping mechanism in highly classified environments, such as government intelligence agencies, research institutions, and financial trading floors. Terrorists, spies, insider traders, prison inmates, identity thieves, and other criminals are using cell phones as a tool to launch attacks, execute illegal activities or compromise information. Detecting — and more importantly, locating — cell phones and other wireless devices helps companies and government agencies protect their assets and prevent unauthorized communications.

AirPatrol's Wireless Locator System provides the actionable intelligence network administrators need to confidently manage cell phone threats and enforce bans on cell phones. AirPatrol greatly simplifies and dramatically lowers the cost-of-deployment of cell phone detection technologies to less than half of the cost of traditional solutions and enables sensor technology to be integrated into existing network infrastructure, rather than being deployed as a parallel network with a discrete overlay security strategy. Once deployed, administrators can manage the environment from a single easy-to-use console that is capable of concurrently displaying all cellular, 802.11 and broadband radio devices.

AirPatrol continues to deliver the market leading advancements customers require to mitigate a broad range of wireless threats—including breakthrough solutions for interference locationing and cell phone detection. AirPatrol's innovations allow enterprises to take advantage of an increasingly mobile world and protect traditional IT infrastructure against wireless-enabled attacks, including those arising from the widespread use of cellular devices.

About AirPatrol Corporation

As the most trusted authority on wireless threats to wired and wireless networks, AirPatrol Corporation delivers the security and network management capabilities today's businesses and government agencies require to solve the industry's most pressing wireless security and network management issues. By offering a comprehensive suite of wireless threat management solutions, AirPatrol enables entities to keep pace with the expanding requirements of a mobile world while complying with pertinent regulations and protecting communications, critical information, and IT infrastructure against present and future wireless threats. Customers and partners include leading network infrastructure and wireless vendors, Fortune 100 enterprises and high-profile government agencies around the globe.

For more information about the contents of this white paper, AirPatrol Corporation products or our company, please contact us at info@airpatrolcorp.com or call us at +1-866-430-4227.