

Volume 2, Issue 1: First Quarter 2010

How Technology Can Make Us Vulnerable

Contents

- Cell Phones Are Safe... Aren't They?
- What Would You Do?
- Meet the Experts: Billy Green
- Meet the Experts: Kevin McQuade
- News Highlights
- What's Wrong With This Picture?

News

12/22/2009
USO Troop Movement Event

12/15/2009
RMA Awarded Contract with Social Security Administration

12/5/2009
RMA Completes Assessment for UNC-Wilmington

12/1/2009
RMA Partners with Clark Nexsen for NCSU Project

10/16/2009
ACCFO Fall Conference

10/12/2009
Disaster Planning Forums

10/8/2009
Bill Booth and Pat King Present at IFMA Conference

10/2/2009
USO of NC Salute to Freedom Gala

9/21/2009
Christine Peterson Wins Movers & Shakers Award

Cell Phones Are Safe... Aren't They?

Imagine this scenario: You're unavoidably called out of town for the week, and are reluctantly forced to delegate the operation of a meeting with some important clients to Bob, an employee who, despite his best efforts, is less than "tech-savvy." Everything seems to be going swimmingly though, and the meeting is set to begin on time. Just before everyone takes their seats, Bob notices an unidentified cell phone lying on the floor of the conference room...



Continued on page 2

What Would You Do?



While traveling on company business, Bob uses a laptop containing company information. When he returned after his last visit, his laptop could not be found. He remembers using it in the airport, but he does not know where the laptop is now.

Continued on page 4

Meet the Experts

Billy G. Green, Jr. M.Ed., CPP, CHS
Security Consultant
Security professional since 1967

What do you enjoy most about your role in security?

I like to think through threats that face us as individuals and companies, define practical countermeasures to confront these threats, and plan actions that may be required if the preventative countermeasures do not work, always "preparing for the worst and hoping for the best."

Continued on page 5

Meet the Experts



Kevin M. McQuade
Security Consultant
Security professional since 1979

What is your greatest security concern?

One of my biggest concerns is that the days of "Oh, that won't happen here" are gone.

Continued on page 6



News

9/11/2009

RMA Awarded Contract from
Naval Facilities Engineering
Services Command

7/21/2009

RMA Awarded Project for Ivy
Tech Community College

7/20/2009

Morton Berkowitz Appointed to
Advisory Board of USO-NC

7/1/2009

Wake County Breaks Ground on
New Mental Health Facility

Cell Phones Are Safe... Aren't They?

Imagine this scenario: You're unavoidably called out of town for the week and are reluctantly forced to delegate the operation of a meeting with some important clients to Bob, an employee who, despite his best efforts, is less than "tech-savvy." Everything seems to be going swimmingly though, and the meeting is set to begin on time. Just before everyone takes their seats, Bob notices an unidentified cell phone lying on the floor of the conference room. Unconcerned, he decides the phone has been misplaced, puts it on an end table, and begins the meeting. No big deal, right? Wrong. Though many of us may never consider it, cell phones represent a significant operational security vulnerability.



Cell phones are active transmitters that use a nationwide network and have the ability to transmit any conversation to any other cell phone anywhere in the United States. The length of a transmission can be practically indefinite, limited only by the life of the power sources on the respective phones. As a result, any cell phone in proximity to sensitive conversation should always be considered a potential vulnerability from both technical surveillance and operational security perspectives.

From a technical surveillance standpoint, cell phones are extraordinarily convenient tools for eavesdropping. Everyone carries cell phones, so a person simply having one in his or her possession is rarely cause for suspicion. If a cell phone being used to eavesdrop on a sensitive conversation is discovered, the perpetrator can always maintain that the phone was simply lost or misplaced.

Additionally, the integrity of all the participants in any secure or sensitive discussion can never be absolutely assured. The larger the group, the more likely it is that even a legitimate participant has divergent or subversive motives. If this is the case, the ability of a cell phone to transmit sensitive conversation to another phone or to a basic recording device as simple as a home message recorder is a serious security risk.

Cell phones can also be compromised by the clandestine installation of software that enables the phone to be accessed remotely without the knowledge of the user. In effect, this activates a "bug" that is unknowingly introduced into a seemingly secure environment by a legitimate participant. This usually requires that the perpetrator of the intelligence-gathering activity have possession of the target phone for some brief period of time in order to make these operating modifications.

However, the more sophisticated the cell phone, the more vulnerabilities it presents. Smart phones with email and Internet capabilities are susceptible to malicious software like viruses in the same way that computers are. While smart phones can pick up malicious software from general Internet browsing, they are also vulnerable to malicious attachments or programs embedded in email or even text messages. Malicious software can make a smart phone vulnerable to remote command, which can allow intelligence gathering parties to intercept phone conversations or even use a smart phone as a remote-controlled eavesdropping transmitter.

The operational security threat posed by the vulnerability of smart phones to malicious software is substantial in that it can allow perpetrators the ability to download messages and other files contained on the phone to a remote site. Sophisticated identity thieves are using this technology every day in criminal enterprises.



From an operational security perspective, there is always the risk of inadvertent activation of a cell phone by the legitimate user in a secure environment. This is commonly known as a “butt dial.” While this type of call may not be as critical an incident as a deliberate third-party interception, it can produce a dangerously random breach of confidentiality depending on whose phone is called in the accidental activation. The use of a speed dial feature requires that only one or two buttons be pushed to cause a dial-out and complete a call.

Bluetooth devices offer smart phone users a convenient, direct, remote audio link with their phones. However, they also represent a significant vulnerability by providing another viable way for malicious software to be introduced into a smart phone. Bluetooth technology also offers the capability for a parallel communications link to be opened with a user’s device without the user’s knowledge. Even if the Bluetooth is password protected, this second, parallel channel under the control of an eavesdropper can be used to activate a smart phone, or to download information and files from it. Specialized criminal systems have been confiscated that scan for Bluetooth links in public places, detect and identify active links with Bluetooth devices, and then download information from those devices. While Bluetooth technology offers users convenient operation of a smart phone, it poses a significantly higher potential for security breaches.

Security Recommendations:

If you’re going to let Bob run your meetings, make sure he doesn’t allow any cell phones or smart phones into sensitive areas. Tell him to inform board members or senior staff that this is not meant to impugn the integrity of anyone present, but to prevent the vulnerabilities related to the devices, which are often unknown to their owners and users, from becoming a significant risk for security breaches.

To avoid the theft of sensitive information through means of malicious software, make sure Bob and his fellow employees don’t store sensitive communication, information or contacts in their smart phones.

Additionally, tell any personnel dealing with sensitive matters that require secure communication not to use Bluetooth devices.

What Would You Do?

While traveling on company business, Bob uses a laptop containing company information. When he returned after his last visit, his laptop could not be found. He remembers using it in the airport, but he does not know where the laptop is now.



Your first thought may be “fire Bob,” however, the most effective way to address this problem is to take action before Bob leaves for his trip.

- First, develop company policies on the proper security procedures when using company laptops, PDAs (Blackberry or iPhone), or portable drives (jump drives, thumb drives, USB drives).
- Train all employees on these procedures and provide refresher training and updates when needed.
- Limit the amount of sensitive information on the hard drive or device, and do not create or keep any “password” files listing usernames and passwords.
- Keep in mind that all information accessed by the device will be stored locally in some fashion, so clean out cache and temp files on a frequent and regular basis.
- Always carry the laptop in the same fashion in the same bag in the same place every time so you will be less likely to accidentally lose it.
- Do not carry a laptop without the benefit of a bag or a case where it can be seen as an easy target by a thief.
- Most airlines now have rules prohibiting placing the laptop in the back pocket of the seat in front of you, and storing the laptop in the overhead bins means it will be out of your control and could be out of the plane by the time you realize it is missing, especially if you are in the window seat.
- Be cautious of people intentionally or unintentionally reading over your shoulder.
- Consider disabling the caching of emails from the company email account on the laptop because if the laptop is lost or stolen, all emails will be lost available on the laptop.
- If traveling employees share a laptop, delete the user account from the laptop when it is returned and use software to wipe all unused areas of the hard drive.
- Any laptop used by an employee should have corporate antivirus software installed and updated on a regular basis.
- The IT department or staff should review, update, and monitor any computer used for company business on a regular basis.

After the loss is determined, immediately contact the last known location to determine if the laptop has been recovered. Even if the laptop can be located, once the loss is reported it should be determined, in an interview with the employee, what was on the laptop. Any password typed into a program, Internet Explorer, virtual private network (VPN), or Remote Desktop connection can be collected from the stolen computer. All passwords on any account used on the laptop should be changed immediately, network wide. It may even be necessary to temporarily disable the account of any person who used the laptop while assessing the magnitude of the potential loss. In addition, all employees who have ever used the laptop should be notified in case they used the computer to access the company network or personal accounts such as email and online banking. Depending on the type of business conducted from the laptop, it may be necessary to notify customers.

Meet the Experts

Billy G. Green, Jr. M.Ed., CPP, CHS

Security Consultant
Security professional since 1967



Family: Wife, Vivian Tilley; stepson and daughter-in-law, Jay and Abigail; grandchildren: Dublin, Collins, and Westin

Education and Experience: Bachelor of Arts, Economics and Business Administration, North Carolina State University.

Master of Education, Adult and Community College Education, North Carolina State University. Post Graduate Studies,

Training and Development, North Carolina State University. Raleigh Police, SBI and FBI National Academies. Former Patrolman with the Raleigh Police Department. Former Special Agent, NCSBI, criminal investigator, intelligence analyst, bomb disposal technician, tactical team sniper and breacher, Supervisor of the SBI Training Division, electronic intelligence and counterintelligence, protection agent and security planner.

Personal Interests: Boating, fishing, reading, terrorism-bombs-explosives-firearms, travel, spending time at the creek (Onslow County) and on the mountain (Ashe County), enjoying adventures with and spoiling the grandchildren.

Certifications: Certified Protection Professional – Board Certified by ASIS International. Certified in Homeland Security Level III (ACFEI). Licensed Counterintelligence Service in North Carolina. Licensed Private Investigator in North Carolina. Secret Security Clearance, US Department of Defense.

Affiliations: American Society for Industrial Security (ASIS). International Association of Bomb Technicians and Investigators (Charter Member). FBI National Academy Associates. Society of Former Special Agents of the NC SBI. American College of Forensic Examiners Institute (ACFEI). Phi Kappa Phi. National Rifle Association (Life Member). Friends of the NC Maritime Museum (Beaufort).

What do you enjoy most about your role in security?

I was a Boy Scout. I learned life-long skills and attitudes in Boy Scouting, one of which is “Be Prepared.” This served me well as a career law enforcement officer and I think it has continued into my second career in security consulting. In his outstanding essay titled On Sheep, Wolves and Sheepdogs, Col. Dave Grossman (US Army Ranger and psychology professor at West Point) defines society as being made up of these three types of people. I identify with the “Sheepdogs.” I like to think through threats that face us as individuals and companies, define practical countermeasures to confront these threats, and plan actions that may be required if the preventative countermeasures do not work, always “preparing for the worst and hoping for the best.” I get great personal gratification and satisfaction from doing what I can to protect the flock from the wolves.

What is your greatest security concern?

The basic principle of CPTED is ‘defensible space.’ This is the same as the basic premise of political sovereignty, that of defined borders. Both correlate with the basic animal and human instinct of territoriality. Subsequently, I consider defined, enforceable perimeters and associated access control to be fundamental to general security and my greatest concern. Controlling people, admitting the authorized and excluding the unauthorized, is more necessary than ever. Whether we are talking about pilfering of laptops by uncontrolled visitors, homicidal assault in a workplace, a domestic violence incident, or terrorists placing an explosive, chemical or biological device, effective control of people at the boundaries is the most fundamental countermeasure.

Meet the Experts

Kevin M. McQuade

Security Consultant
Security professional since 1979



Place of Birth: White Plains, New York

Education and Experience: Wake Technical Community College, Electronics Diploma. Training in various security systems including TAC-INET and Continuum, Pelco Endura and Integral, CSI, Casi-Rusco, and NCS. AGC Sales/Negotiations Skills Training Course. Dale Carnegie Sales and Recurring Monthly Training Courses

Personal Interests: Enjoy golfing and spending time with my wife either at home relaxing or away on weekends.

Affiliations: Member of ASIS International.

What are some notable or memorable projects?

One of the most memorable projects that I have been involved with at RMA is when we were contracted by a large fortune 500 company to oversee the entire security management system from the owner's perspective. The company had offices that were part of this Security Management System in over eight states in the beginning and expanded over time through mergers and acquisitions. We were not involved with any installations, just the day to day operation of the system that included policies and procedures on the use of the access badges and card reader portals, periodic clean-up of the card database, writing specifications on the programming requirements and following up and testing the equipment on new installations. We were also involved with the individual user groups within the company on a daily basis assisting them with badge replacements for employees, new hires and on-going training. There were four full-time personnel involved with this position when it began, and over three years, it grew to ten full-time employees located in four states. Another project that is most memorable is the design of the new Security Management System for the North Carolina School of Science and Mathematics in Durham. The school had a security management system, however the functionality of the system was such that it was not expandable or able to integrate to other systems. The new system is now a complete security management system integrating card access, digital video, emergency communications and an IP-based emergency paging and intercom system throughout the entire campus. The school also implemented a new security console with multiple workstations and video displays that monitor the security, video, and emergency communications for the entire campus.

What do you see as a future, emerging trend in security?

I believe that more systems will have the capability of integrating with each other and will also utilize a more secure wireless technology.

What is your greatest security concern?

One of my biggest concerns is that the days of "Oh that won't happen here" are gone. Not everyone has realized this yet, and some do not take the proper precautions to avoid potential risks, especially in "quiet" cities, towns, or areas of the country. Everyone needs to be more conscious of their surroundings whether it is at work, home, on vacation, in the car, or at the grocery store. I think we have become too complacent and the "good old days" are not like they used to be. This is not to say we need to have our guard up at all times or live our lives in fear; we just need to be more conscientious.

News Highlights

July 2009: Wake County broke ground on a new inpatient mental health facility, and RMA will provide Project Management services related to the integrated security management systems during the construction phase of this project. Morty Berkowitz was appointed to the Advisory Board of the USO of North Carolina and will provide assistance in developing an outreach program and other public relations duties. RMA was awarded a project to provide Safety and Emergency Services Consulting Services to Ivy Tech Community College in Indiana.

September 2009: RMA was awarded an IDIQ (Indefinite-Delivery Indefinite-Quantity) contract to provide the Naval Facilities Engineering Services Command (NAVFAC) with Anti-Terrorism Force Protection Engineering Services. Christine Peterson was selected as winner of the sixth annual Movers & Shakers Award from Business Leader Media.

October 2009: The USO of NC honored six outstanding members of our Armed Forces at the "Salute to Freedom Gala," and RMA together with Phyllis Eller-Moffett of Quality Staffing Specialists, Mercedes Auger, Brian Goldsworthy, and Trish Mercer of Travel Experts, contributed over \$5,000.00 to the USO of NC at the event. Bill Booth and Pat King presented *Dealing With Threatening Situations: How to Keep the Worst From Happening* at IFMA's World Workplace 2009 conference. Two Disaster Planning Forums were hosted by Risk Management Associates, Highlands Environmental Solutions, and Ward and Smith, P.A., and moderated by Catalyst Communications. RMA attended and was a vendor participant at the 2009 Fall Conference of the North Carolina Association of Community College Facility Operations (ACCFO).



ACCFO Fall Conference

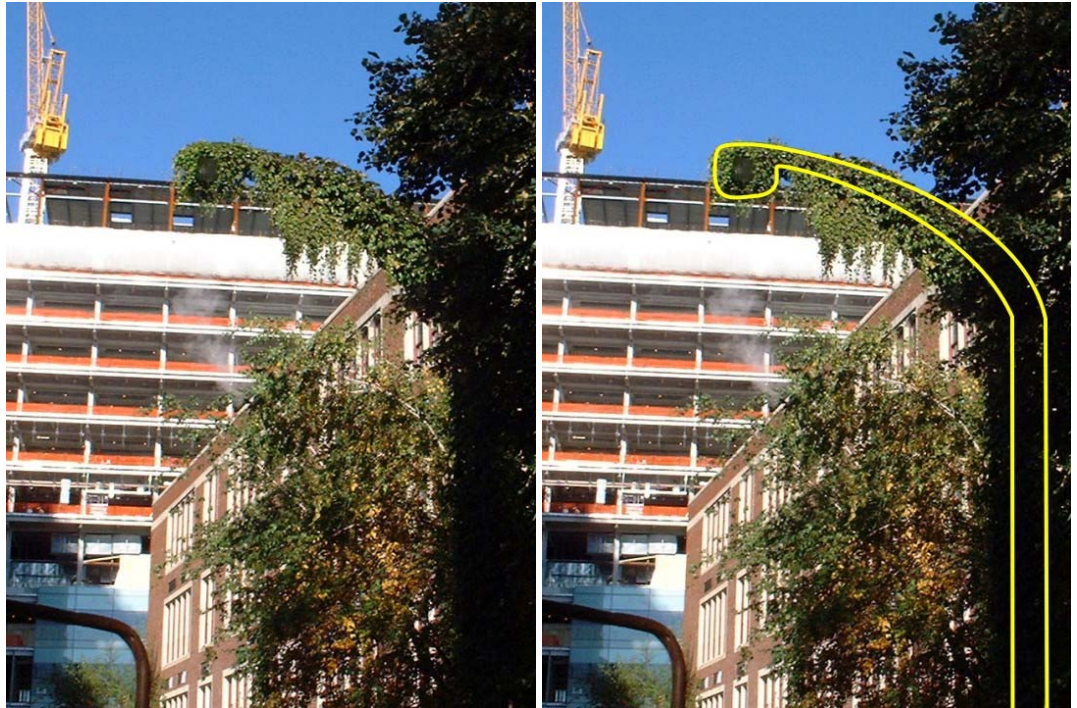
December 2009: RMA has partnered with Clark Nexsen for the design of North Carolina State University's non-woven pilot facility. RMA completed an Outdoor Physical and Environmental Security Assessment for the Main Campus of the University of North Carolina at Wilmington. RMA was awarded a contract to provide an Equipment Specialist for the Social Security Administration's (SSA) Office of Facilities Management's (OFM) Office of Protective Security Services (OPSS) Division of Security Operations and Policy (DSOP). RMA staff assisted over 200 service men and women at Raleigh-Durham International Airport in support of the USO of North Carolina during a troop movement.



USO Troop Movement Event

What's Wrong With This Picture?

Can you find the hidden light fixture?



Can you find the hidden predator?



Risk Management Associates, Inc.
4000 WestChase Blvd. Suite 350
Raleigh, NC 27607
Phone (919) 834-8584
Fax (919) 834-8150