

## Volume 2, Issue 2: Second Quarter 2010

Protect Your Assets. Know Your People.

### Contents

- Pre-employment Background Investigations
- What Would You Do?
- Meet the Experts: Darren Nix
- Meet the Experts: Wayne Truax
- News Highlights

### News

4/14/2010  
Goddard Space Flight Center Training

3/11/2010  
Fraud Lunch and Learn with Womble Carlyle

2/16/2010  
RMA Conducts Theft Investigation for Non-Profit Organization

2/15/2010  
RMA Awarded Project for United Developers

2/12/2010  
RMA Facilitates the Recovery of over \$7 Million in Assets

2/7/2010  
RMA Provides Security Services and Computer Forensics Assistance to Orange County Superior Court

2/4/2010  
Smith Anderson Lunch and Learn

2/3/2010  
RMA Conducts Theft Investigation

### Pre-employment Background Investigations

**Why Did the Chicken Cross the Road?** You know the rhetorical question and the answer: to get to the other side. But would the chicken cross a six-lane highway during rush hour traffic with his eyes closed? I think not; chickens are smarter than that. I use that old joke to illustrate the dangers and risks some companies assume if they have no policy for conducting thorough pre-employment background investigations before allowing new employees access to their assets.



[Continued on page 2](#)

### What Would You Do?



John entered his office, dropped his bag on the floor, and began sifting through the piles of paper on his desk that never seemed to shrink. On top of the pile was the P/L from the previous month that he had been scrutinizing late the night before. He frowned as he noticed an entry for a payment to a vendor he did not recognize. As he looked through the reports before him, an uneasy thought began to creep into his mind. Was something wrong happening here?

[Continued on page 4](#)

### Meet the Experts

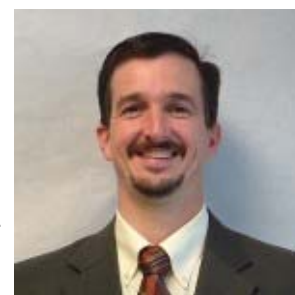
#### Darren A. Nix, CPP

Senior Associate  
Electronic systems and security professional since 1988

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

I think the primary and constant trend in the last seven or eight years has been how much more versed people are with respect to security. It's easy to recognize convergence of physical and IT security, the developments of networked video recording, IP-based card readers and cameras, and the continued growth of smartcard technology.

[Continued on page 7](#)



### Meet the Experts



#### Wayne Truax

Security Consultant/Investigator  
Law enforcement and security professional since 1970

#### What do you enjoy most about your role in security?

I enjoy the investigative role of my job as I see it benefiting the client immediately. Normally as a result of the investigative effort, we make recommendations that will deter or prevent incidents from happening again.

[Continued on page 8](#)



## News

1/31/2010

RMA Completes Safety and Emergency Preparedness Study for Ivy Tech

1/19/2010

RMA Awarded Blast and CBRNE Vulnerability Assessment Project

1/16/2010

Kevin M. McQuade Earns Certified Protection Professional

1/15/2010

RMA Awarded Technical Editor Position

## Why Did the Chicken Cross the Road?

You know the rhetorical question and the answer: to get to the other side. But would the chicken cross a six-lane highway during rush hour traffic with his eyes closed? I think not; chickens are smarter than that. I use that old joke to illustrate the dangers and risks some companies assume if they have no policy for conducting thorough pre-employment background investigations before allowing new employees access to their assets. Why would a company knowingly put their physical, intellectual, and human assets at risk? There seem to be three different perceptions. First, owners or managers assume they will be able to make the best hiring decision for their company even though their decision may be based on limited, incomplete, and possibly fraudulent information. Second, they think that thorough pre-employment background investigations are simply too expensive and fail to see the ROI. Finally, many just haven't thought it through.

It is human nature to make decisions we feel are in our own best interests. The problem for you as a manager or owner is that potential employees frequently make decisions in their own self interest that are contrary to yours and those of the business. Any decent writer can create a falsified résumé. A Google search of "fake résumés" produces 4,560,000 hits. The first site on the list was [www.fakeresume.com](http://www.fakeresume.com), which stated that more than 53% of job seekers and 70% of college graduates lie on their résumé. The website offers guidance in "filling gaps," "finding foolproof methods to add experience," attaining "fake references," and getting "transcripts from *any* university with *any* GPA you want." It even suggests that if a candidate doesn't lie, hiring managers will *assume* they have. For many, rhetoric like this is reason enough to invent. The chances of encountering a falsified résumé are substantial, and without proper security measures, you could become a victim.

### The costs associated with hiring the wrong employee are frightening.

Mindboggling statistics have been published by security, HR, accounting, auditing, risk management, business and economic organizations. Here are some recurring figures:

- 35% to 60% of job applicants have inaccuracies and/or misrepresentations of some sort on their résumés/applications
- Internal theft and fraud cause nearly 30% of business failures
- 70% of these internal theft or fraud crimes are committed by repeat offenders
- The cost of employee theft to employers is between \$60 to \$120 billion a year
- One bad hiring decision can cost more than \$100,000, not including the costs associated with theft, violence, harassment, or wrongful termination

### What is the bottom line?

It is simply smart business to gather the necessary information to make a good hiring decision. Obvious reasons aside, good hires provide a competitive advantage to a company by increasing morale, sending a positive message to other employees and making people more productive. A poor hire can do just the opposite. Either way, managers and owners are expected to know whom they are hiring and whether this person is the right fit for the organization. In addition, studies show companies who have pre-employment background investigation policies:

- Attract higher quality applicants,
- Discourage applicants with something to hide,
- Have better and more complete information on which to base hiring decisions,
- Reduce company liability by showing due diligence,
- Encourage applicants to reveal "true self",
- Comply better with applicable federal and state mandates, and
- Provide a safer work environment.



### **So you want to know more about proper hiring strategies?**

Résumés are a tool employers use to identify individuals who meet the requirements of the position they are trying to fill. Applications are the tool employers use to fill in the gaps résumés leave, and should require candidates to attest to the truthfulness of the information they have provided on their résumé. Applications should also include an “authorization and disclosure statement,” requiring a signature that permits background investigation for the purpose of employment and stating their rights under the Fair Credit Reporting Act. Standard applications that meet state and federal guidelines are available from various sources. HR directors and legal representatives can typically provide you with pertinent additional information.

The goals of a pre-employment background investigation are twofold: to verify that the information given is accurate and complete and to look for information that has been omitted for reasons that are unfavorable to the applicant. To be effective, companies should require that the application be completed in full to include all applicable addresses and contact information, dates of attendance, employment, residences, and other information. It is important that qualified personnel review the application for completeness and follow-up on any missing data or gaps.

Most employers look back seven to ten years on applicants, but there are some instances where longer historical investigation is appropriate. At a minimum, the background investigation should include Social Security number verification, birth date verification, current and former address history, employment history, reference and developed reference verification, and criminal records checks. These measures provide any employer with the verification and validation needed to support the information gathered from the résumé and interviews. Additional important information includes the verification of education, civil records (including bankruptcy), state licensing, credit reports, military records, regulatory sanctions, sexual offender indices, terrorist lists and driving records.

It is perfectly reasonable for a company to complete all or portions of pre-employment background investigations themselves if they have the resources in house. In some cases Risk Management Associates works alongside companies who check references and former employers. Other companies depend on us for all of their records checking. Using an outside service is a good fit for companies who do not have the experience and/or resources to perform a thorough investigation in-house. It also puts an additional layer of liability protection between the company and the applicant and can often be a cost savings. Either way, the most important thing to remember is that thorough pre-employment background investigations are imperative to providing the necessary information for making the best hiring decision for your company. Like the chicken, it helps to see if danger is coming.

"Review your hiring procedure to ensure that a thorough background screen and criminal history check is conducted on all potential employees, especially those who will have access either to trade secrets, or to the private information of employees or consumers. After all, the best defense to the would-be rogue employee is not to hire him in the first place. Part of this screen should include asking for and thoroughly checking references, which we find is all too frequently omitted by companies, but which provides an excellent source of information (or perhaps equally telling, a lack of information) about the applicant. Companies may consider more thorough screenings for employees handling sensitive information. In addition, with the proliferation of social networking pages, it can be useful to conduct an Internet search to see if the applicant has elected to provide additional information about him or herself online." *Privacy & Security Law Report, ISSN 1538-3423*

## What Would You Do?

*Note: The following paragraph is an amalgamation of several recent RMA cases. Names and circumstances have been modified, combined, or altered to protect the privacy of our clients.*



John unlocked the front door of the office and headed straight for the break room for his second cup of the day. A plate of homemade cookies sat next to the coffee, and he realized that Jane must already be at work. Her dedication to the job was admirable, yet she always seemed to find time to do those extra things that made people feel special. On his way back to his office, he noticed a birthday gift on Mary's desk. Jane must have left that as well. John entered his office, dropped his bag on the floor, and began sifting through the piles of paper on his desk that never seemed to shrink. On top of the pile was the P/L from the previous month that he had been scrutinizing late the night before. Usually Jane handled the details, but with the way the economy had been, he felt the need to take a closer look. Some of the documentation looked a little off, and he reminded himself to ask Jane yet again for the relevant files. Finance and accounting were not his strengths, and he relied on her to run that part of the business and explain it to him when needed. Last month, however, something just seemed off. Income was slightly down, but the expenses seemed strangely high. John sighed, fearing that he would have to deny employee requests for raises for a third time. He frowned as he noticed an entry for a payment to a vendor he did not recognize. There was another, and another, and the amounts seemed a little high. As he looked through the reports before him, an uneasy thought began to creep into his mind. Was something wrong happening here? He dismissed the thought as irrational paranoia. The only person with enough skill was Jane, and he trusted her implicitly. This was a small business, and they were like family here. He dug through his desk and found the reports for the previous two months. They had the same pattern, and his uneasiness grew. What if Jane had been stealing from the company?

Unfortunately, the scenario described above is not unique or unusual. Employee theft and embezzlement has always been a problem, especially for small businesses, and some experts believe the problem may be increasing in today's economy. RMA has recently assisted several clients with this problem. Although not comprehensive, the information below is intended as a starting point to recognizing and preventing embezzlement.

### What conditions make embezzlement easier?

- **Little to no oversight, especially of a trusted employee.** Oversight could be provided by an immediate supervisor, a supervisor at a higher level, or an outside third party such as an accountant or auditor. In addition to making embezzlement more difficult, oversight provides an opportunity to examine the standard accounting process for errors or inefficiencies. In our recent cases, the thefts were discovered by supervisors taking a closer look or by new employees learning the process.
- **A large amount of available petty cash.** Petty cash should be kept to a minimum for several reasons, not just potential misuse. Simply from a security standpoint, it may be unwise to have a large amount of cash in an unsecured office or desk. Allowing employees to have access to ready cash is sometimes too tempting to resist. Company credit cards are a good alternative to petty cash and provide an opportunity for oversight when reconciling the statements. If petty cash is used, receipts should be mandatory and the reconciled frequently. One of our recent cases involved a significant manipulation of petty cash.

- **A trusted employee in a family atmosphere.** This seems like an ideal situation, but no employee should ever be trusted to the point where their work is not subject to evaluation and scrutiny. Speaking from personal company experience, our Vice President has been the model of integrity for our company since she started in 1991. She has Secret clearance from the Department of Defense and is our Facility Security Officer. She is beyond reproach, and her trust is not questioned. Although she is responsible for all accounts payable and payroll, the bank statements are only opened and reviewed by the company President who provides oversight of the process. In our recent cases, the thieves were highly respected members of the organization who were thought to be incapable of embezzlement.

#### **What are some common characteristics of the thief?**

- **An exceptionally dedicated employee.** Working late or arriving early provides an opportunity to work without supervision. By never taking a vacation, the thief reduces the chance of discovery by a replacement. An employee who volunteers to go to the bank to conduct transactions on behalf of others may be hiding a crime. Each of our recent cases involved a suspect who used at least one of these methods.
- **Someone who seems to live beyond their means.** The thief is spending the money they should not have in ways that are not typical. This could be gifts, sometimes lavish or expensive, for family, friends, and coworkers. The embezzled money could be spent on the home, clothing, or furnishings, or on vehicles including cars, boats, RVs, ATVs, or similar items. Sometimes the thief may lend money to family or a friend in need. If questioned, this unusual freedom with money is often explained as an inheritance or other unexpected windfall. Although each suspect spent their ill-gotten gains in different ways, all shared a common trait of spending more money than they seemed to have.
- **A person with a history of embezzlement or other issues.** If they have stolen once, chances are they will steal again. With new employees, the first line of defense is a pre-employment background investigation. Some previous incidents of embezzlement may not have resulted in criminal prosecution, making a civil record search for anomalies even more important. In addition, previous employment references may provide direct information or indirect clues about the circumstances surrounding the termination of employment. Of our recent cases where the employee was a relatively new hire, the thief had been suspected of embezzlement at a previous employer. No pre-employment background investigation was conducted.
- **Someone who is everyone's friend.** The thief may be trying to avoid suspicion by making sure that everyone thinks highly of them. If someone is your friend, you find it harder to believe that they would steal from you. They may also be trying to solicit help from unknowing accomplices to manipulate some part of the system over which they have no control. This could involve requesting "help" on the computer to "fix an error" or requesting assistance on an unusual task. The suspects in our recent cases were described as friendly, well-loved members of the organization.
- **A person who routinely operates outside the system, especially related to computer software.** Many companies operate using an accounting system or software that requires some form of modification. It is understood that certain changes are required to meet the needs of the business, for example if an error needs to be corrected or an entry needs to be legitimately changed. Frequent changes and "fixes" provide opportunities to insert fictitious "fixes" to hide embezzlement. All of our recent cases have involved a suspect who manipulated the accounting software to hide their embezzlement.

#### What can a company do to minimize the risk?

- **Provide internal oversight and review.** Many companies have some form of control in place, but these controls must be periodically evaluated for appropriateness, effectiveness, and compliance. Require two signatures on checks, and do not allow the use of a signature stamp on checks. When reviewing information, do not just skim the information and “rubber stamp” the process. If something seems suspicious or unusual, ask questions and investigate. The thieves in our recent cases all took advantage of a lapse in internal oversight.
- **Provide external oversight and independent evaluation.** An outside auditor or accountant providing review services will make embezzlement more difficult. In addition, outside oversight provides an opportunity to evaluate the entire system and suggest improvements that may benefit the financial situation of the company. As with internal oversight, it provides an opportunity to discuss the function and health of the business as well as future plans for growth. It can be difficult for a small business to hire an outside auditor or accountant, but this service is highly valuable.
- **Create and follow sound policies and procedures.** Companies may create good policies and procedures, but they are useless if not followed or updated as conditions change. As businesses change, processes should change and evolve to meet the needs of the business. If a new vendor needs to be added to the system, for example, require approval from a supervisor to complete this task. When entries are changed, require approval for this process. Separate accounting functions and cross train employees in different tasks to minimize one single person having control of the accounting process. Periodically evaluate the entire accounting process for compliance with established policies and procedures. In all of our cases, the suspect conducted activities considered “normal” that were contrary to written policies and procedures.
- **Use the appropriate tools and technology.** If the accounting software is not appropriate for the company, modify it to make it work without a great deal of manual intervention. Create a process and method for changing entries that produces a record that is examined for accountability. Provide training to employees and supervisors to make them familiar with the abilities and limitations of the system. If not using accounting software, make sure that the paper system is organized, straightforward, and clear. In all of our recent cases, the suspect took advantage of a “glitch” in the system.

If you suspect embezzlement, contact a professional who specializes in addressing those situations. This could be a forensic accountant, an attorney, or an investigative company.

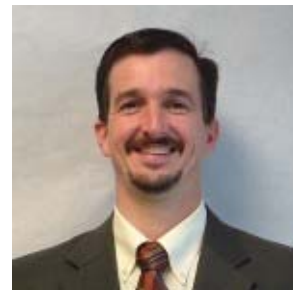
---

## Meet the Experts

### **Darren A. Nix, CPP**

Senior Associate

Electronic systems and security professional since 1988



**Family:** Happily married and proud father of four.

**Education and Experience:** Four years in the US Navy. Received an A.A.S. degree in Aviation Technology and continued working in the Aviation Industry on electronic systems for the next several years. Served as an Operations Manager for a security integrator prior to joining RMA.

**Personal Interests:** Enjoy being involved in church with family, maintaining a 34-acre hobby farm, gardening, hunting, and participating in sports with my kids.

**Certifications:** Certified Protection Professional – Board Certified by ASIS International. Licensed Counterintelligence Service in North Carolina. Licensed Private Investigator Associate in North Carolina.

**Affiliations:** Member of Security Products Magazine Editorial Advisory Board and author of several articles and a web-based TV segment on securing the nation's critical infrastructure. Member of ASIS International. Volunteer firefighter.

### **What are some notable or memorable projects?**

Although my time at RMA has been spent providing services for a variety of clientele in the private and local public sectors, I have concentrated on developing business with the federal government. I was the lead project manager for 16 NASA security projects. Some of the projects included a comprehensive threat and vulnerability assessment of Johnson Space Center and Security Management System design for multiple NASA facilities. I also worked on the OneNASA Smartcard project as a subcontractor to the Maximus/EDS team, providing assessment and subject-matter expertise in the convergence of physical and IT security systems. As a result of some developed relationships over the years, RMA was recently awarded an IDIQ contract with NFESC to provide AFTP (antiterrorism force protection) services. NFESC provides these services to the Navy, Marines and other DOD agencies.

### **What do you enjoy most about your role in security?**

I enjoy being part of a company where I can have a direct impact on success and growth by bringing ideas and working as a team. Ultimately, I enjoy making a difference.

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

I think the primary and constant trend in the last seven or eight years has been how much more versed people are with respect to security. It's easy to recognize convergence of physical and IT security, the developments of networked video recording, IP-based card readers and cameras, and the continued growth of smartcard technology. These have all certainly been trends and continue to grow, but I think one of the biggest trends we are going to see is testing. There are so many reports of technology not working properly when a security event has taken place. The need for accurate testing continues to increase.

### **What is your greatest security concern?**

My greatest security concern is the unknown. We can fairly easily predict the probability of internal theft, workplace violence, vandalism, and other common problems. However, it is extremely hard to predict specific terrorist acts and "practically" develop solutions to mitigate them.

## Meet the Experts

### Wayne C. Truax

Security Consultant/Investigator

Law enforcement and security professional since 1970



**Place of Birth:** Windsor, Ontario, Canada

**Family:** Married to Minnie with three children and six grandchildren

**Education and Experience:** Bachelor of Applied Science, Criminal Justice, Campbell University. Retired from the North Carolina State Bureau of Investigation in 1998.

**Personal Interests:** Salt water fishing and gardening

**Certifications:** Licensed Private Investigator in North Carolina.

**Affiliations:** Member, ASIS International. Member, Society of Former Special Agents of the North Carolina SBI. Member, Order of the Long Leaf Pine.

### What are some notable or memorable projects?

RMA conducted a security assessment for a statewide community college system involving over 23 campuses in 14 regions. We came up with security recommendations that could be tailored to the specific needs of each campus and region. In another case, RMA completed an investigation that resulted in the recovery of over a million dollars worth of equipment that had been hidden by company employees.

### What do you enjoy most about your role in security?

I enjoy the investigative role of my job as I see it benefiting the client immediately. Normally as a result of the investigative effort, we make recommendations that will deter or prevent incidents from happening again.

---

## News Highlights

**April 2010:** RMA developed, updated, and delivered training programs to security and receiving personnel at the Goddard Space Flight Center.

**March 2010:** RMA and Womble Carlyle presented *Enemies at the Gate - or Are They Already Inside?* a seminar on how to prevent, combat, and correct fraud in the workplace.

**February 2010:** RMA assisted in an investigation concerning the loss of product and possible employee involvement at a packaging and distribution warehouse that handles industrial grade paper products. RMA hosted a Lunch and Learn session for Smith Anderson to update the client about the resources available in security and investigations. RMA provided security services and computer forensics assistance to Orange County Superior Court. RMA located and facilitated the recovery of over \$7 million of equipment in a bankruptcy case. RMA was awarded a project to conduct security system design services for the new Bunce East Apartment Community. RMA conducted a theft investigation for a non-profit organization and is currently developing a comprehensive security program to help prevent and deter future thefts.

**January 2010:** Risk Management Associates was awarded a contract to provide a Technical Editor dedicated to NAVFAC ESC in Port Hueneme, California. Kevin McQuade earned the designation of Certified Protection Professional from ASIS International. RMA was awarded a project to conduct a Blast Analysis and CBRNE Vulnerability Assessment for NAVFAC ESC. RMA completed a survey and assessment of the fourteen Ivy Tech Community College regions.

---