

December 2008

# PLANNING *for* CHANGE

## Security Managers' Perspectives on Future Demographic, Crime, and Technology Trends

Nancy G. La Vigne, Ph.D.

Samantha S. Hetrick

Tobi Palmer



**ASIS**  
FOUNDATION™



URBAN INSTITUTE  
Justice Policy Center



**URBAN INSTITUTE**  
Justice Policy Center

2100 M Street NW  
Washington, DC 20037  
*www.urban.org*

© 2008. The Urban Institute. All rights reserved.

The views expressed are those of the authors and should not be attributed to the Urban Institute, its trustees, or its funders.

The ASIS Foundation funded this research.

ISBN 978-1-887056-88-5

## ACKNOWLEDGMENTS

The authors thank all the roundtable participants for contributing their expertise to this report.

**Mr. Shayne P. Bates, CPP**  
Principal Security Consulting  
Koffel Associates

**Ms. Valerie Q. Brumfield, CPP**  
Director of Security  
St. Joseph Medical Center

**Mr. Tommy J. Burns, CPP**  
Director of Security  
Harrah's Las Vegas Flamingo

**Mr. Douglas I. Callen**  
President  
Callen & Associates

**Ms. Linda J. Fite, CPP**  
Director of Security Services  
Fairview University Medical Center

**Mr. Michael D. Gambrell**  
Sr. Vice President of Industry  
and Government Affairs  
Dunbar Armored, Inc.

**Mr. Richard D. Gipson, CPP**  
Director of U.S. Partner  
and Asset Protection  
Starbucks Coffee Company

**Dr. Kenneth R. Grover**  
Vice President of Security  
Darden Restaurants, Inc.

**Mr. Mark L. Guadette**  
Director of Loss Prevention  
Big Y Foods, Inc.

**Mr. Anthony Heredia**  
Director of Investigations  
and Asset Protection  
Target Corporation

**Mr. John D. Horton**  
Director of Security  
Echelon Resorts

**Mr. Gene W. James, CPP**  
Director of Asset Protection  
Jack in the Box, Inc.

**Mr. Kelly S. Klatt, CPP**  
Director of Safety and Security  
Loews Hotels

**Mr. Donald E. Knox, CPP**  
Security Specialist  
State Farm Insurance

**Mr. Ronald Lander, CPP**  
Chief Specialist  
Ultra-Safe Security Solutions

**Mr. Jeffrey S. Levitt, CPP**  
Senior Manager of Asset Protection  
Panera Bread

**Mr. Steven B. Lindsey, CPP**  
Director of Security Services  
Wal-Mart Stores

**Mr. James P. Litchko, CISSP, CAS**  
President and CEO  
Litchko & Associates

**Mr. Thomas F. Lynch**  
Director of Security  
Baystate Medical Center

**Mr. Ronald Martin, CPP**  
Lead Security Specialist  
U.S. Department of Commerce

**Ms. Carol Martinson**  
Vice President, Asset Protection  
SuperValu, Inc.

**Mr. Richard H. McClintock**  
Director of Security  
Dartmouth-Hitchcock Medical Center

**Mr. Kevin McGarr**  
Executive Vice President  
and Chief Operating Officer  
Canadian Air Transportation  
Security Authority

**Mr. James Metzger**  
Counter-Terrorism Coordinator  
SEPTA Transit Police Department

**Mr. J. J. "Mick" Mickelson,  
OCP, CHS-V**  
Global Security Manager  
McAfee, Inc.

**Mr. David Nelson, CISA, CISSP**  
Examination Specialist  
Federal Deposit Insurance  
Corporation

**Mr. Ryan Roberts, CPP, PSP**  
Security Group Manager  
Microsoft Corporation

**Mr. P. Kevin Smith, CPP**  
Vice President  
Chevy Chase Bank

**Mr. Philip W. Stewart, CPP**  
Manager of Special Projects  
Compliance, and Training  
Massachusetts General Hospital

**Mr. Frank R. Torrell**  
Director of Asset Protection  
Dollar Tree

**Mr. Michael H. Weiss**  
Supervisory Special Agent  
Office of Inspector General

# CONTENTS

<b>Executive Summary</b>	<b>1</b>
<b>Section 1. Introduction and Overview</b>	<b>4</b>
<b>Section 2. Methodology</b>	<b>5</b>
<b>Section 3. Demographic Challenges</b>	<b>6</b>
Aging Population .....	7
Youthful Population.....	9
Diverse Population.....	11
Demand for Qualified Security Personnel .....	14
<b>Section 4. Crime Trends</b>	<b>17</b>
Identity Theft and Fraud .....	18
Organized Retail Crime .....	24
Terrorism.....	26
<b>Section 5. Technology</b>	<b>28</b>
Using Technology Creates Opportunities for Crime .....	28
Using Technology to Combat Crime .....	31
<b>Section 6. Special Topics</b>	<b>34</b>
Public Policy and the Law .....	34
Enlisting the Public in Security Efforts .....	35
<b>Section 7. Conclusion</b>	<b>36</b>
<b>About the Authors</b>	<b>37</b>
<b>Appendices</b>	
Glossary .....	38
References.....	42

## EXECUTIVE SUMMARY

The United States security industry faces many challenges, perhaps the greatest of which is the perpetually changing landscape in which security measures are applied. In 2007, the ASIS Foundation contracted the Urban Institute (UI) to forecast demographic, crime, and technology trends in the United States for the next five to 10 years, and provide guidance for the emerging security challenges that may arise from such predictions.

UI researchers compiled published data from a range of sources and held a series of roundtable discussions with security industry experts. These roundtables elicited first-hand impressions, experiences, and recommendations from dozens of security experts representing the banking, health care, hospitality, information technology, insurance, retail, services, and transportation sectors. The key findings stemming from these discussions are outlined below, along with recommendations for addressing these predictions.

**Demographic Challenges.** The U.S. population projections for the next decade include a significant increase in the proportion of older persons (those aged 65 and older) and a more racially and ethnically diverse population.

- As the aging population increases, older persons will remain in the workforce longer. This may provide opportunities for building a more reliable security workforce, as these employees are viewed as more trustworthy. However, security managers should also anticipate some challenges, as older workers are perceived to be less familiar with workplace technologies. Security managers can prepare for this demographic shift by developing technology training tailored to an older population
- By way of contrast, it is believed that the youthful population (18- to 34-year-olds) will possess technological knowledge far above that of their older counterparts. To capitalize on this anticipated strength, security managers should use educational networks to recruit competent young workers into the security industry, and modify hiring practices and training methods to retain these youthful workers over time
- The national trend toward a more ethnically, racially, and geographically diverse population may create future security challenges, including language barriers, culture clashes, and discrimination concerns. Security managers can plan for this increased diversity by establishing guidelines to accommodate other cultures, offering cultural awareness training for all employees, and engendering and embracing a multi-cultural setting

**Crime Trends.** While current violent and property crime rates remain lower than those reported for 2000, fraud—particularly that accomplished through computers and/or the Internet—is predicted to be a growing problem. Other anticipated security threats include violence in the workplace, Organized Retail Crime (ORC), and both domestic and international terrorism.

- In the next five to 10 years, identity theft and fraud will continue to be the fastest growing crimes. However, the nature of identity theft is likely to shift to more organized, high-stakes, global attacks. To prepare, security managers should coordinate and share intelligence with all levels of law enforcement, invest in fraud detection systems, comply with standards for storage of sensitive data, and when possible, eliminate frequency cards
- The increase in the share of older Americans will also likely lead to personal victimization (i.e., fraud, identity theft, and confidence scams) due to their relative inexperience with technology
- Anticipated increases in the ethnic and racial diversity of the United States are likely to create more culture clashes and conflicts that can threaten security and lead to more workplace violence
- ORC will continue to grow and become one of the most costly crimes experienced by the security industry. Efforts should begin now to train employees on identifying behaviors associated with ORC activities. Security managers should also improve relationships with law enforcement to encourage collaboration and develop reporting protocols
- The threat of a terrorist attack will remain a serious security issue. Security professionals will be challenged to protect likely future targets, particularly soft targets such as public places, food supplies, and electrical grids. Security managers could benefit from considering terrorism prevention in the context of crime prevention and from implementing flexible and adaptable response management plans
- Another terrorist attack will likely spur demand for security personnel. This need will increase the challenges security managers already experience hiring qualified employees and obtaining sufficient security clearances. To assist with these obstacles, security managers should develop better working relationships with law enforcement and human resource departments, and engage in efforts to further professionalize the security field

**New Technologies.** Security managers should expect a continued proliferation of new technological advances, which will both create opportunities for crime and present new ways of enhancing security.

- In the coming decade, more widespread use of the Internet, as well as increased reliance on information systems, will make private information more vulnerable to access and manipulation by criminals. Security managers should focus on reinforcing measures to protect both public and private information systems, get ahead of the curve by attending hackers' conventions, and engage in ongoing computer network penetration exercises
- Technological advances will provide new and more effective ways of enhancing security efforts. Emerging technologies that security managers should consider investing in include video analytics, automation, and counterintelligence information systems

The final section of the report examines topics that security experts raised, as well as common themes discussed across sectors. While these do not pertain directly to future demographics and crime trends, these issues are concerns for security managers as they look toward the future. Topics include concerns with public policy, laws, and industry regulations, some of which create compliance challenges or conflict with sound security measures. Security experts also recommended enlisting the public in security efforts as a critical and often overlooked strategy.

As the security industry looks ahead toward its next 10 years, security professionals are challenged with adapting current protocols and technologies, and developing new ones in response to emerging demographic and crime trends. In anticipation of these changes, leaders in the security industry could take a more proactive role anticipating likely impacts, facilitating conversations around these issues, and planning and advocating for changes that offset threats outlined in this report while capitalizing on the benefits. This approach holds promise for achieving significant gains for the safety and security of employees, consumers, and the public.

## Section 1

# INTRODUCTION AND OVERVIEW

Over the past few decades, the security industry has made great advances promulgating industry standards, developing new technologies to address existing concerns, and adapting to new social realities. Despite these developments, few systematic reviews exist that document future demographic, crime, and technology trends. Even scarcer are studies that explore how such trends might guide the industry toward measures that anticipate and offset security threats, while capitalizing on trends that might enhance and improve the industry's effectiveness. To address this issue, the ASIS Foundation contracted the Urban Institute, a nonprofit, non-partisan social policy and economic research organization, to conduct a study on how various industry sectors can better prepare for emerging security issues.

Specifically, this research set out to:

- Learn how demographic, crime, and technology trends vary based on industry sector and security threat
- Determine what these trends suggest about future security challenges, investments, and resource needs
- Identify promising strategies and tactics the security industry can adopt or enhance in preparation for anticipated industry developments

Guided primarily by the perspectives of security experts, this report provides concise descriptions of predicted demographic, crime, and technology trends in the United States, summarizes how experts anticipate these changes will influence security over the next five to 10 years, and offers practical recommendations for security managers to adopt now to address these anticipated trends.

The report is divided into three sections by key topic areas: demographic challenges, crime trends, and technology. The final section addresses issues that surfaced during discussions, which are indirectly related to the ability of security professionals, business executives, and workers to prepare for a safer environment for employees, clients, and customers.

While this publication is tailored to security managers, it will also be useful to a wide array of personnel, including public sector employees, such as local and federal law enforcement.

## Section 2

# METHODOLOGY

In September 2007, the UI convened six roundtables of security experts to elicit their perspectives on how future demographic, crime, and technology trends would affect security issues in their industry sectors, and to offer recommendations on best preparing for these anticipated changes. Participating security experts, selected from the ASIS membership directory with guidance from ASIS Foundation staff, represented the following sectors: banking, insurance, retail, transportation, services, hospitality, information technology, and health care.

UI examined data collected from sources relevant to this project (e.g., Federal Bureau of Investigation, Census Bureau, and Federal Trade Commission documents). Overall, the available demographic trend data revealed that the American population is becoming older and more diverse. The crime trend data showed that fraud is a major security issue across all sectors. UI researchers developed industry-specific roundtable questions based on these general themes to guide discussions.

Prior to the roundtables, participants were provided with the future trends forecasts and discussion topics concerning three basic concepts: (1) current security issues within each sector; (2) challenges of demographic, crime, and technology trends; and (3) ways to better prepare for anticipated security issues. Participants were asked questions such as:

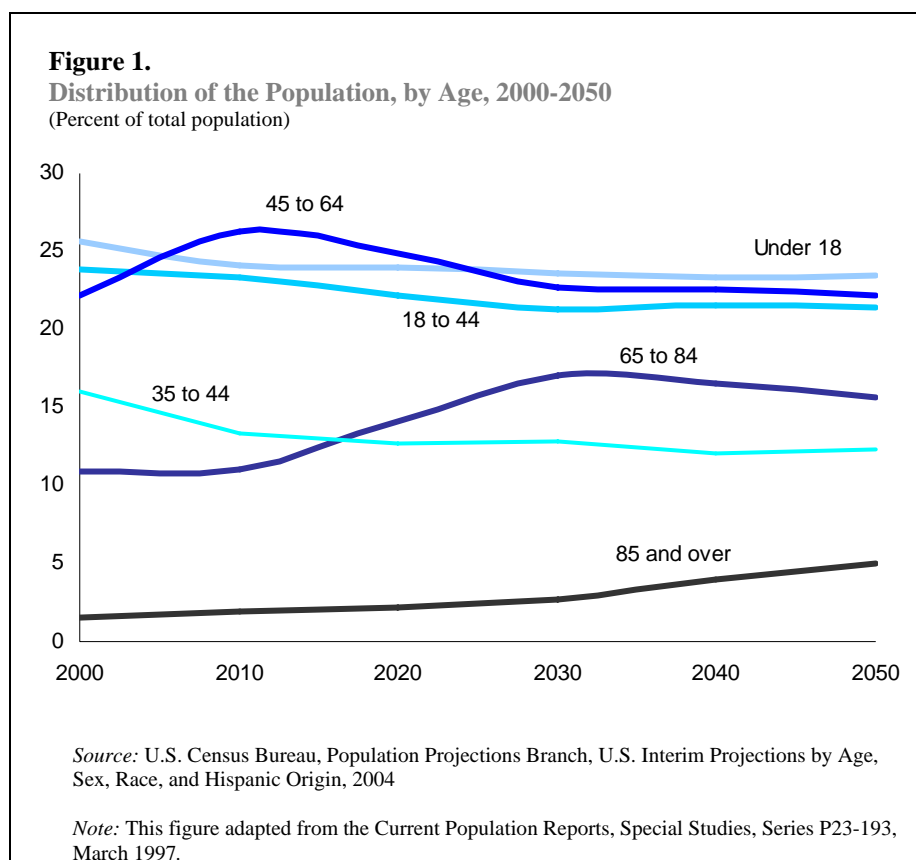
- In your view, what will be the most pressing security issues for your organization and your industry in the next five to 10 years?
- Trend data reveal that the population will become older and more diverse—how do you anticipate these changes will influence the security goals for your organization and the larger industry?
- Crime trends suggest a continued increase in fraud and identity theft. What do you feel are the best methods to combat these crimes?

Each section of this report begins with a discussion of the published data, followed by synthesized perspectives of the security experts, and concludes with topic-specific recommendations developed by UI after analyzing the published data and roundtable results. UI staff documented the roundtable discussions, highlighted major themes, and synthesized information across sectors. These findings are organized by type of anticipated demographic, crime, and technology trend in the remainder of this report.

## Section 3

# DEMOGRAPHIC CHALLENGES

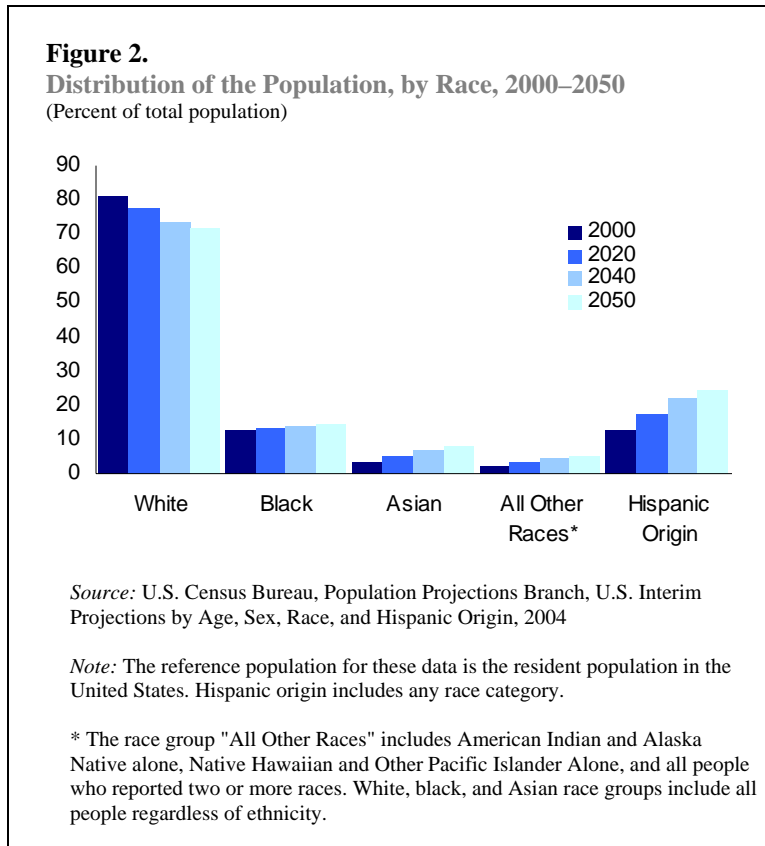
According to the U.S. Census Bureau (2000), major demographic changes anticipated in the coming decade include an increase in the share of older Americans and a more racially and ethnically diverse society. This trend will continue for more than 40 years, with the proportion of persons over the age of 65 steadily increasing and those under the age of 65 gradually decreasing. The 65- to 84-year-old group (11 percent of the population in 2000) will experience the most significant increase, with the highest proportion (17 percent) projected for 2030 (figure 1). The middle-aged group (45- to 64-year-olds) is expected to have the most marked decrease, with a projected negative change of 4 percent in the coming years.



The highest peaks in each decade are likely a reflection of the aging baby boom generation. For example, the year with the largest proportion of 35- to 44-year-olds (16 percent) was 2000. Every 10 years, the next age group experiences its highest proportion. By 2050, those aged 85 years and over are estimated to represent 5 percent of the population, whereas the same age group represented less than 2 percent of the population in 2000.

In addition to the aging of the U.S. population, society is predicted to become more racially and ethnically diverse. As shown in figure 2, white Americans are the only group that is estimated to decrease, while all other races, as well as those identifying themselves as Hispanic, will experience gradual growth over the next few decades. Asians and the “All Other Races” group (American Indian, Alaska Native, Native Hawaiian, Other Pacific Islander, and those reporting

two or more races) will nearly double as a group between 2000 and 2050. The percent of the population identifying as Hispanic, will increase from 12.6 percent in 2000 to a predicted 24.4 percent in 2050, nearly doubling in size.



In the following sections, we document the views of security industry experts on how the demographic shifts for the next five to 10 years, along with characteristics of the youth population, are expected to influence their specific sectors.

## Aging Population

By far the most drastic demographic change on the horizon is the aging of the population. Security experts from the transportation, health care, banking, and insurance sectors indicated that this increase would have a dual impact on the workforce. On one hand is the anticipated workforce shortage, as an increasing number of people retire. Indeed, given the large volume of employees retiring today, many industries are already struggling to replace staff and will continue to face this challenge in the future. On the other hand, security experts expect a greater reliance on older persons to fill positions. According to some transportation security experts, organizations are already deliberately revising their hiring practices to recruit more retired persons. We expect this trend to continue and become more pronounced in the coming decade.

## *Older Workers*

According to several security experts, training, communication, and the ability of older persons to perform their jobs safely and efficiently will become increasingly important. The ability of older workers to fulfill job requirements will be greatly influenced by the type of industry and specific job demands. Some hospitality and services experts felt that an older workforce could be detrimental, as many positions in their industry are physically demanding. Retail security experts expressed concerns about the safety of older workers on the job and feared an increase in the number of employee deaths in the workplace (e.g., due to heart attack or stroke) as well as increases in workers' compensation claims. In addition, many security experts believe older workers lack the technological knowledge that their younger counterparts possess.

Despite these challenges, employing older workers also has benefits. Security experts noted that generally older workers demonstrate a stronger work ethic and better people skills than their younger counterparts. Older workers are viewed as highly valued employees for their reliability, maturity, and ethics, with many experts expressing concern that the departure of older people from the workforce may create security challenges. Many experts noted that older employees could serve as role models for their younger counterparts. More specifically, those from the hospitality and service sectors observed that older employees are more apt to take security protocols seriously, and their people skills are an asset in defusing tense situations.

Nonetheless, with an anticipated increase in the share of employees over the age of 65 working side-by-side with others in their 20s, communication problems will arise and so will differences in each group's understanding of security issues. One example provided by information and technology experts was that older workers, who are accustomed to filing documents away in a metal cabinet with a lock and key, might have discomfort in an environment where most documents are processed and stored electronically. However, experts acknowledged that as the population continues to age, computer literacy among older employees would increase with time.

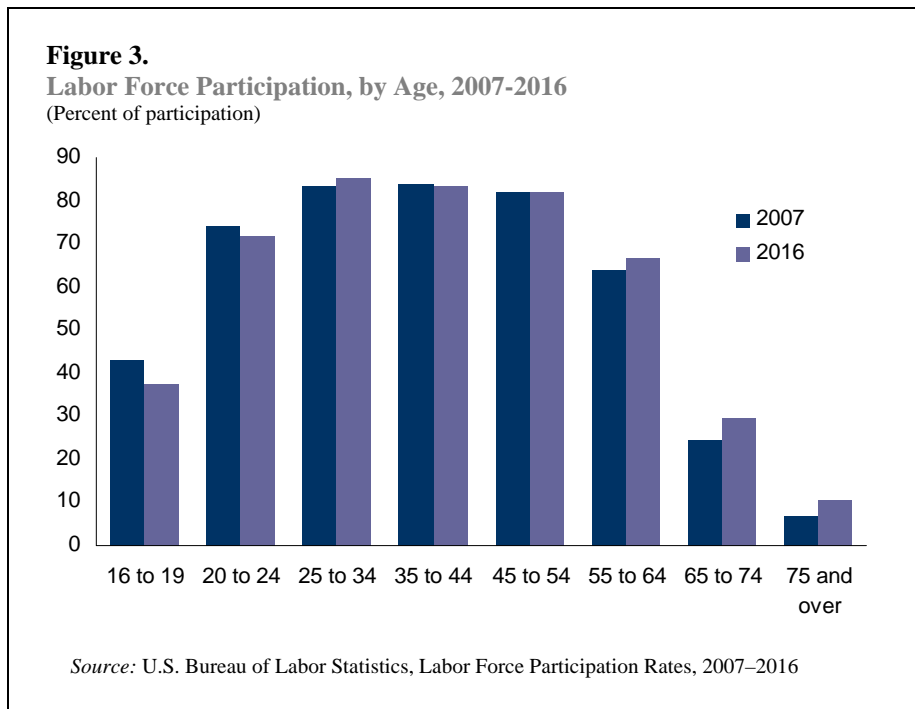
### **Recommendations:**

- Provide specialized training to help older workers better understand new technologies and their uses in the workplace
- Include ways to establish better communication between older and younger workers in all employee-training efforts
- Standardize employee and management training and deliver it across all positions and levels so that all employees are aware of what to look for and how to respond to security issues

## Youthful Population

Although the share of younger Americans in the workforce is expected to decrease, we predict their participation, coupled with the predicted growth in older Americans, will significantly widen the generational gap between these two groups of employees. The U.S. Census Bureau projects that the percentage of 16- to 24-year-olds participating in the labor force, 60 percent in 2007<sup>1</sup>, is expected to decrease, and continue to be one of the smallest age groups contributing to the workforce (figure 3). On the other hand, older Americans, who are living longer, healthier lives, will continue working for longer periods of time, adding unique challenges associated with a potential 50 year age gap in the workplace.

Representatives from all industries predicted that this widening of the generational gap could have both positive and negative impacts. Security experts observed that younger workers are generally less likely to exhibit the value system and work ethic typically found with older workers. However, the technological knowledge of the younger generations is, and will continue to be, tremendously valuable.



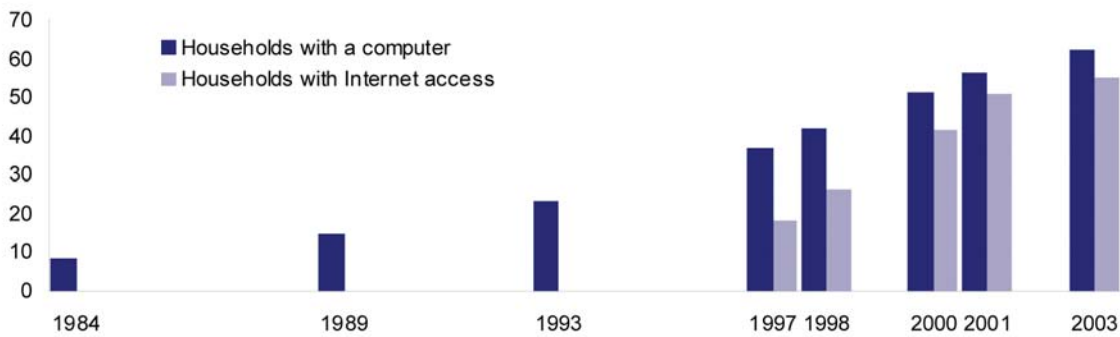
### *Technological Knowledge*

Across all sectors, security experts observed that younger workers possess a deeper understanding of newer technologies compared to older workers. This may be attributable to the increasing percentage of households with a computer and Internet access, as well as the increased use of the Internet for entertainment and business activities (figure 4). While this knowledge is beneficial, it is likely to create difficulties when younger workers communicate with or learn from older counterparts. Encouraging effective communication and interaction

<sup>1</sup> U.S. Bureau of Labor Statistics, Labor Force Participation Rates, 2007-2016.

between these two groups is critical. Security experts felt that efforts should be made now to facilitate a shared understanding of security issues and strategies between older and younger generations. In addition, security issues and methods of protection should be incorporated into college-level curricula (such as criminal justice and business courses) to help educate students in advance of their entry into the workforce.

**Figure 4.**  
Percent Households With a Computer and Internet Access, 1984-2003



Source: U.S. Census Bureau, Current Population Survey, 1984, 1989, 1993, 1997, 1998, 2000, 2001, 2003

Note: No data available for missing years. This figure adapted from Current Population Reports, Special Studies, Series P23-208.

Along the same lines, security experts noted differences between older and younger workers' preferences for training and communication methods. Younger generations tend to be comfortable using digital documents and devices, while older workers are generally more comfortable and accustomed to paper documents. Indeed, given their extensive use of computer games, MP3 players, and cell phones, most youths today have a basic knowledge of common technologically based communication tools. Security experts cautioned, however, that while security systems are increasingly being developed with these preferences in mind, youthful workers must also be schooled in hands-on security measures, which continue to be necessary within the electronic age. Security managers should take actions now to educate older employees regarding newer technologies while also safeguarding more traditional hands-on protocols.

### ***Values and Ethics***

Security experts noted that the advantage of younger workers being technologically savvy is a double-edged sword. They observed that in general, younger workers tend to have underdeveloped value systems and appear to lack a strong work ethic. This is exacerbated by the ease with which they operate in the digital world, in that they may treat electronic information as being less valuable and more open to manipulation. We therefore predict greater workplace challenges due to the blurring of the boundaries between "right" and "wrong" that will lead some youth to justify unlawful acts such as hacking, illegal downloading of digital information, and infringing copyrights.

Additionally, some security experts expressed concern that in the future, younger workers will be less willing to work their way up through the ranks. Experts noted that in the past, working for

the same company from youth through retirement was the norm. That is a rarity today, and job tenures are likely to become shorter with young people changing employers rather than staying with one company. As one expert noted, workers traditionally chose employers based upon a company's reputation; in the future, younger workers will likely select employers based on their salary structure and compensation packages. This shift in criteria may lead to less loyalty among youthful workers. Security managers should consider ways in which they can invest in their younger employees now to engender more loyalty and longer tenures. For example, one significant employment barrier concerns tattoos and body piercing, which are prohibited in many security jobs. One expert suggested that in order to be competitive in the future, prohibitions based on such elective physical attributes should be revisited.

### **Recommendations:**

- Standardize training and education using communication methods that promote both hands-on and technological knowledge of security issues
- Create mentoring programs to ensure institutional knowledge is passed down to younger employees
- Utilize educational networks to encourage the integration of business, criminal justice, and security programs into a security management degree
- Invest in employees to engender a sense of loyalty, thereby increasing job retention and promoting longer tenures
- Develop hiring standards based on qualifications rather than physical appearance

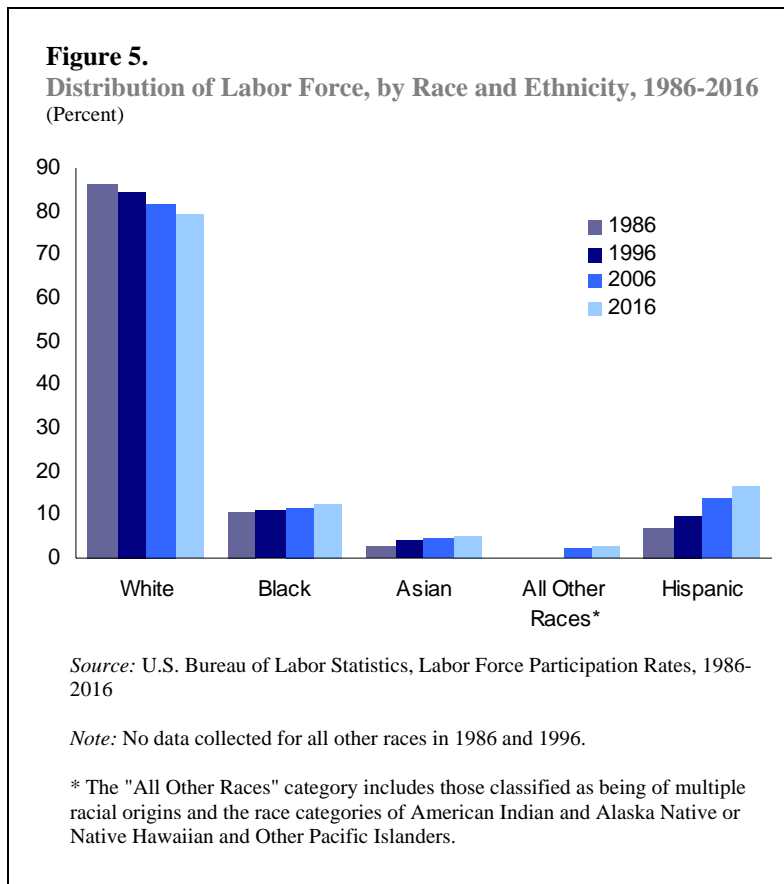
## **Diverse Population**

We now turn to a discussion of expected shifts in the racial and ethnic composition of the U.S. population, which is predicted to become more diverse in the coming years. Indeed, over the past several decades the U.S. Census Bureau's demographic projections of foreign-born and native populations reveal that the only racial category on the decline is that of non-Hispanic whites. All other racial and ethnic categories (as well as Hispanic-origin populations) are expected to rise, creating an increasingly diverse population.

Although the number of non-Hispanic whites in the labor force will continue to increase with the population growth, the proportion of whites in the workforce is expected to decrease (figure 5). In contrast, the share of other minority racial and ethnic groups (including blacks, Asians, and Hispanics) will rapidly increase and constitute a larger share of the labor force.

The Census Bureau also projects an increase in the share of foreign-born residents, with 12 percent of the population being foreign-born by 2020 (figures 6 and 7). Additionally, the 2000 Census estimates that foreign language use within the United States has increased, with 18 percent of the population speaking a non-English language at home (up from 14 percent in 1990). The growth in non-English speaking populations extends beyond Spanish speakers (60 percent of those speaking a non-English language) to include Indo-European, Asian and

Pacific Island languages. The most frequently spoken languages other than English and Spanish are Chinese (2 million), French (1.6 million), and German (1.4 million).<sup>2</sup>



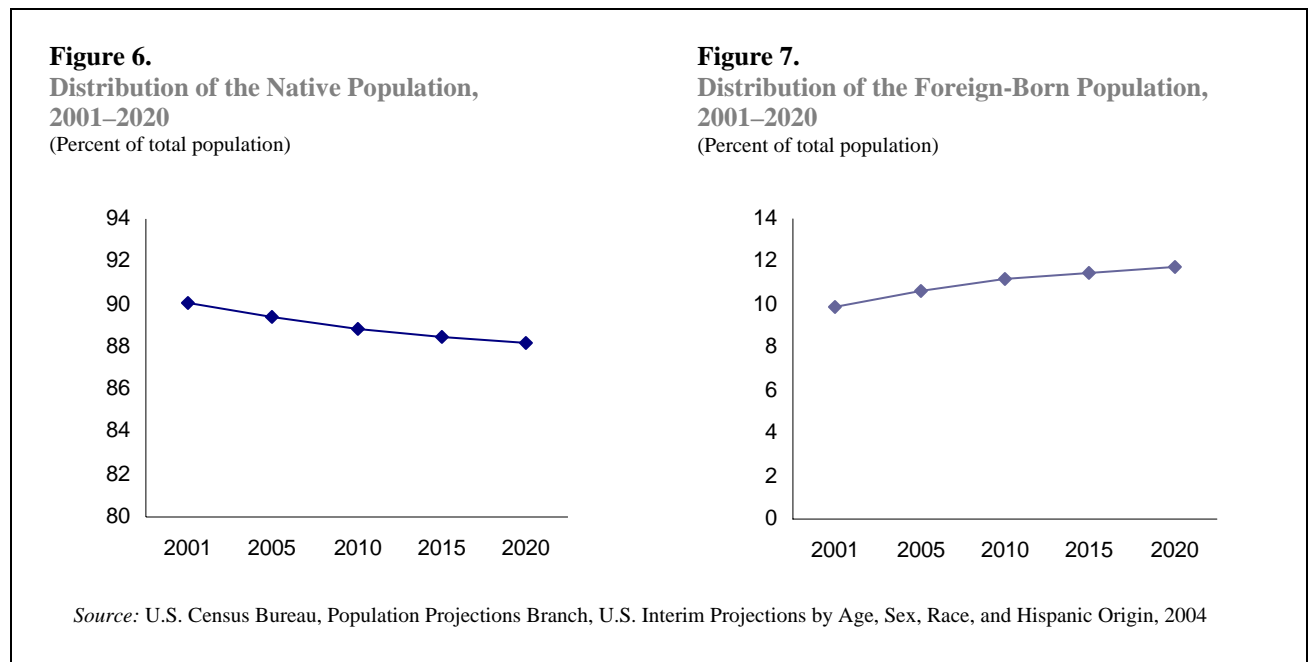
The U.S. Department of Labor reports that in 2007, foreign-born individuals comprised nearly half of the increase in workforce participation. According to security experts, this increase in cultural diversity creates both opportunities and challenges. On one hand, the growing diversity will bring individuals who can assist with language barriers that are of increasing concern, particularly among those in the retail and health care sectors. However, this new and more diverse group of workers may also create the need to adapt current security measures and accommodate different cultures in ways that were not necessary in the past.

### ***Employment Practices***

With the blending of cultures in the workplace, many security experts predict that hiring practices, workplace attire, employee schedules, language requirements, and job practices will need to be revised. With regard to hiring practices, recruitment of foreign-born individuals tends to take significantly longer than native-born applicants, due to the extensive security clearances that are required and the length of time to conduct thorough background checks. Once the hiring process is complete, employee dress codes and schedules may present additional obstacles. For example, some job candidates may encounter problems with workplace attire or uniform requirements, which restrict the use of religious garments. Many security experts believe these

<sup>2</sup> Statistics presented in this paragraph were obtained from the 2000 Census brief on language use and English-speaking ability. <http://www.census.gov/prod/2003pubs/c2kbr-29.pdf>

dress codes will need to be revised to accommodate cultural and religious practices, while still ensuring security needs are met. Similarly, experts advised that it would be important to recognize employees' religious holidays and to adjust schedules accordingly.



The increase in the share of foreign-born residents will be accompanied by an increase in the number of non-English speaking clients (figures 6 and 7). According to security experts, one of the biggest issues concerning cultural diversity will continue to be language barriers between staff and clients. For example, current health care policy mandates the availability and use of medically trained translators for proper communication of medical procedures and treatment to non-English speaking patients and their family members. The increasing variation in both culture and language is a strong incentive to ensure employees are as diverse as the clients they serve. In addition, non-native speaking employees may require additional cultural awareness training, which will be critical for effectively communicating with a diverse population.

### ***Workplace Victimization and Discrimination Concerns***

While the increased diversity of the population could create opportunities for improved communications between staff and clients, security professionals expressed concern that this mix of cultures might increase opportunities for workplace violence. Security experts reported that differing views among cultures explain much of the crime and victimization that already occurs in their industries. Some retail security experts noted that culture clashes and racial tensions can trigger aggressive behavior, which in turn, increase incidences of violence.

Concerns about appearing to discriminate against minority or foreign-born employees also create security challenges. Security experts anticipate a heightened awareness of possible racial discrimination and a greater reluctance to employ certain security measures due to fears that they may be misinterpreted and prompt legal action. As one security expert noted, failure to accommodate for cultural differences could be viewed as a violation of constitutional rights. The tension between equal treatment and adequate security also applies to prospective clients. Security experts from the banking and insurance sector noted that foreign-born clients might

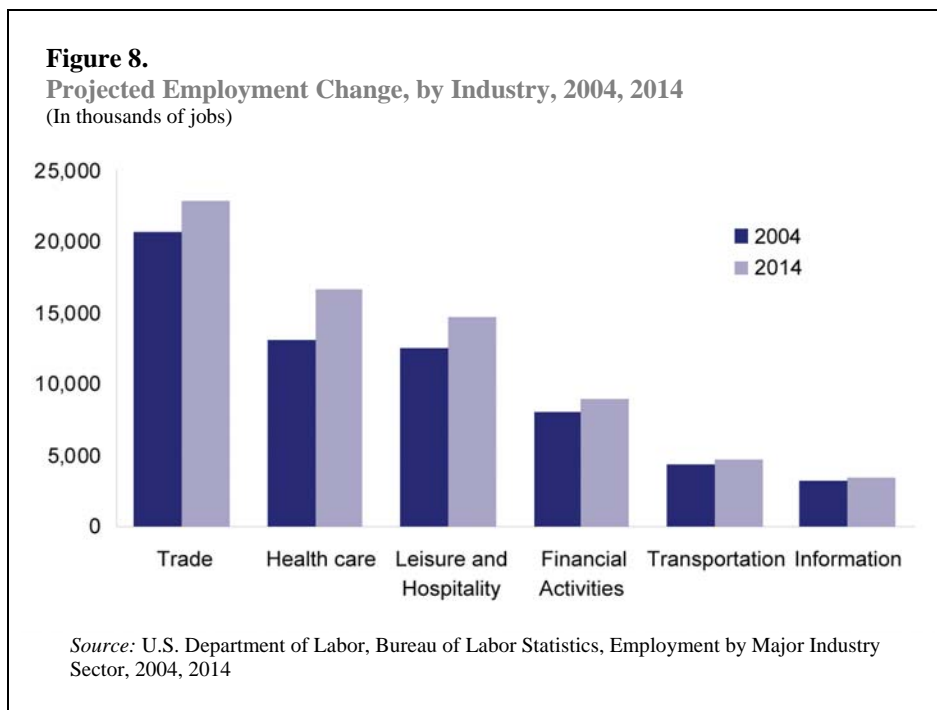
avoid cash transactions because of personal information that by law, must be disclosed. Clients might perceive these disclosure requirements as being invasive, which could instill fear and damage the company’s relationship with the public. Similarly, the more extensive security clearances required for employing foreign-born applicants might be perceived as a form of discrimination.

**Recommendations:**

- Require or help employees learn English and establish guidelines for accommodating other cultures and origins
- Diversify the workforce and engender a multicultural setting. Revisit regulations to ensure they accommodate the increasing diversity of employees
- Advocate for cultural awareness within the community and workplace to avoid misperceptions and reduce the likelihood of discrimination

**Demand for Qualified Security Personnel**

One common theme that emerged from roundtable discussions was the challenge in hiring qualified security professionals. As shown in figure 8, the size of the workforce in each major industry sectors is projected to grow in the coming years, with trade and health care experiencing the most significant increase. Given the heightened focus on homeland security issues following the terrorist attacks of 9/11, the demand for qualified security personnel has become particularly acute. Even line-level security positions require specialized knowledge, generating greater demands for people with specific technical skills. Security professionals will likely need to resort to even more outsourcing to meet staffing needs.



## *Contract Security*

While experts anticipate an increased reliance on contract security companies, many cautioned that not all these organizations conduct sufficiently thorough background checks. Security experts for the banking and insurance sectors were particularly concerned, and emphasized the importance of verifying information provided by prospective contract employees. In the words of a transportation security expert, a background investigation is not simply about criminal history checks, but should also include an examination of the applicant's country of origin, residential history, and career trajectory. For example, an applicant applying for an entry-level security position whose previous employment history reveals an expertise in electronic circuitry should raise a red flag.

The growing reliance on contract security employees may also increase the probability of internal clashes within organizations. Security experts voiced concerns about how contract employees, by the very nature of their status, might become a divisive factor within the corporate culture of an organization. Some may perceive them as not being a part of the company, and that can result in a lower level of commitment to the organization on the part of the contractor.

The hiring of contract security employees could also raise questions about adequate compensation. Contract employees are costly to hire due to fees paid to agencies, yet the employees themselves tend to receive lower levels of compensation than their salaried counterparts. Transportation security experts expressed concerns that the relatively low compensation offered to security officers restricts the caliber of the candidates they are able to attract. For example, one participant said it is unrealistic to expect people who are paid minimum wage to vigilantly monitor CCTV cameras and to approach their jobs in a professional and thorough manner. If security managers are to plan effectively for the future, they will need to consider ways to adequately compensate both contract and in-house employees.

## *Personnel Screening Practices*

Security experts predicted that increased demand for security personnel would place additional pressures on human resource departments, which they say are already doing a questionable job adequately screening candidates. It is believed that it takes too long to conduct credit checks and many screening practices lack thorough background investigations of prospective employees. Several experts contended that insufficient screening of employees is likely the source of much workplace internal theft, a problem that could increase as demand for new personnel increases.

These problems are anticipated to become even more acute in the event of a new terrorist attack. If the events of 9/11 are any indication, a subsequent attack will cause yet another hiring flurry. Security managers observed that, whereas past recruitment efforts relied heavily on law enforcement veterans, police departments are less likely to be the source of future security labor because apart from homeland security functions, police workforces are on the decline. Several experts noted that increased hiring demands might lead to a lowering of standards for employment and inadequate background checks. Security experts said much could be done now to avoid this outcome, recommending the establishment of background investigation standards and a wholesale professionalizing of the industry. However, experts cautioned that attempts to apply such standards would likely face obstacles. Several experts expressed difficulty obtaining background information on potential employees from both federal and state databases because privacy regulations restrict sharing this information with entities outside of law enforcement.

Even when background information can be shared legally, experts noted that local law enforcement agencies often lack the resources to fulfill requests in a timely manner.

### ***Partnerships with Law Enforcement***

A related issue is partnering with law enforcement to aid in investigations and prosecutions. Many security experts anticipate that in the future, the dual pressures of homeland security and routine policing will make law enforcement less able to collaborate with private security. Experts contended that law enforcement may be less inclined to partner given that the most common types of crimes are misdemeanors, which do not merit the effort it takes to build a case for prosecution. While some security experts felt that they did not have good working relationships with local police departments, others were more optimistic about future partnerships, citing existing collaborations.

### **Recommendations**

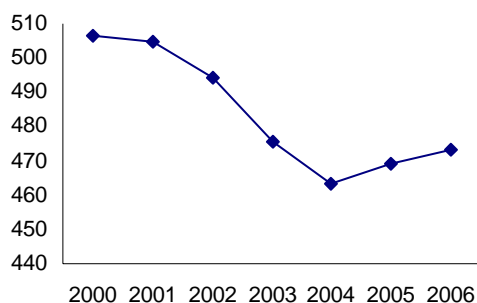
- Develop working relationships with the human resources department and local law enforcement agencies. Be proactive about providing solutions for existing needs and discuss how to overcome future obstacles
- Collaborate with security professionals both within and across industries. This symbiotic relationship will alleviate security issues on a broader scale as well as capitalize on the strengths and resources of all professionals
- Increase the professionalism of the security field by establishing standards for employment with educational requirements and certification

## Section 4

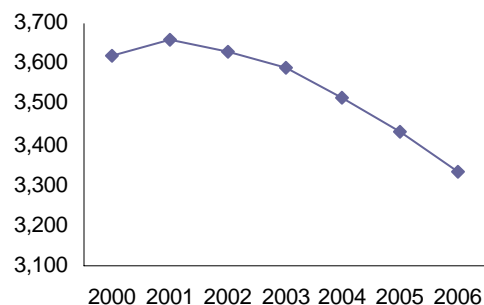
# CRIME TRENDS

Both violent and property crime in the United States have been falling precipitously in the past several years (figures 9 and 10), with only a more recent uptick in violent crime. Despite these gains in public safety, the degree to which crime rates will remain low is uncertain. Increases in violent crime have already been observed between 2004 and 2006.<sup>3</sup> The current state of the economy, with mortgage foreclosures at record highs, suggests that both property and violent crime will soon be on the rise.

**Figure 9.**  
Violent Crime in the United States,  
2000-2006  
(Rate per 100,000 inhabitants)



**Figure 10.**  
Property Crime in the United States,  
2000-2006  
(Rate per 100,000 inhabitants)



Source: Federal Bureau of Investigation, Uniform Crime Reports, 2000-2006

In addition, the incarceration and release of criminal offenders is predicted to continue to grow, and resource-strapped state and local governments may be unable to provide the programming, treatment, and services necessary to prevent released prisoners from reoffending.

The implications of these worsening economic conditions may explain why security experts anticipate increases in identity theft and fraud,<sup>4</sup> violence in the workplace,<sup>5</sup> Organized Retail Crime, and terrorism. While several of these trends are more prevalent in one industry than another, considerable overlap exists in many of the issues raised by the security experts.

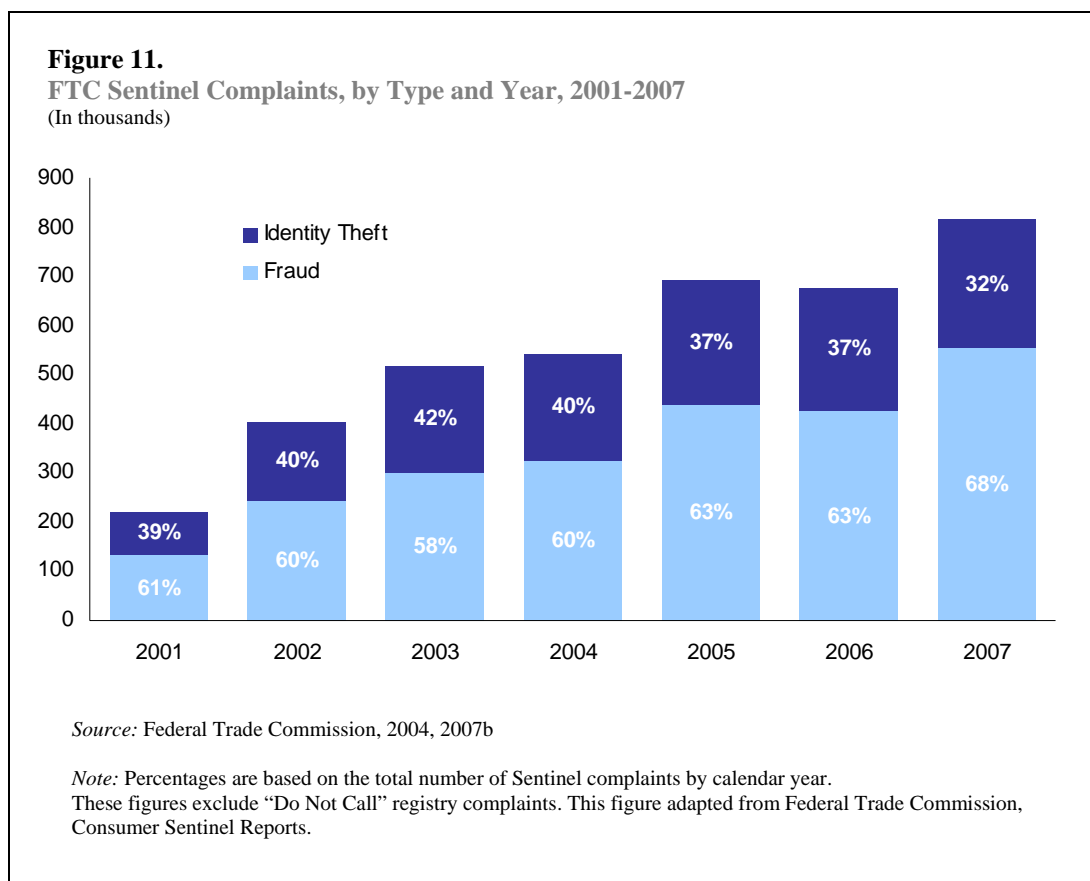
<sup>3</sup> Preliminary statistics released by the FBI indicate that both violent (-1.4) and property (-2.1) crime decreased when compared with data from 2006 (U.S. Department of Justice 2008b).

<sup>4</sup> Identity theft and identity fraud are terms used to describe types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically, though not always, for economic gain (U.S. Department of Justice 2008a).

<sup>5</sup> Violence in the workplace is a broad term and can be grouped into four categories: 1) violent acts by persons with no connection to the workplace; 2) violence directed at employees by customers, clients, patients, students, inmates, or any others for whom an organization provides services; 3) violence against co-workers by a present or former employee; and 4) violence committed in the workplace by someone personally connected to an employee (Rugala and Isaacs 2004).

## Identity Theft and Fraud

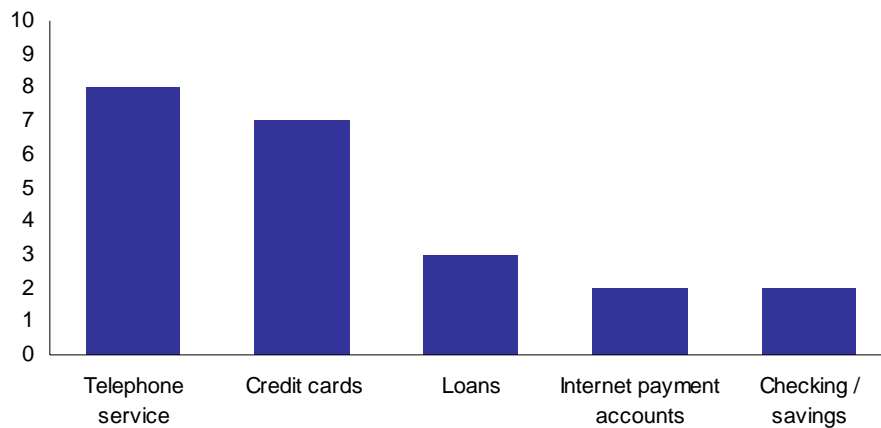
The Federal Trade Commission (FTC) reports that each year approximately eight million people are victims of identity theft, with estimated losses totaling \$15.6 billion (FTC 2007a). In addition, identity theft is the fastest growing financial crime and potentially the fastest growing crime overall (Hoar 2001). Identity theft complaints rose from 86,212 in 2001 to 258,427 in 2007 (FTC 2008) (figure 11). The FTC cites several methods used to obtain personal information including: taking documents or bills from garbage or mail; stealing credit card numbers; phishing<sup>6</sup>; diverting billing statements to another address; stealing wallets, purses, and personal records; bribing employees with access to personal information; using false pretenses to obtain personal information from financial institutions or telephone companies; and hacking into network systems or personal computers to access personal information (FTC 2008).



The FTC found that the types of accounts most often compromised are: credit cards (61 percent), bank accounts (33 percent), and telephone service accounts (11 percent) (FTC 2007). Stolen information is typically used by thieves to open new accounts, often credit card or telephone accounts; provide police with false identification when stopped or charged with a crime; obtain medical treatment, services, or supplies; secure housing; and obtain government benefits or employment (figure 12) (FTC 2007). Not surprisingly, most identity theft victims (84 percent) did not know their offender and many (74 percent) do not report the crime to police (FTC 2007).

<sup>6</sup> “Phishing” refers to the use of e-mails designed to lure users to false sites and extract personal or confidential information from them (Federal Trade Commission 2006).

**Figure 12.**  
**New Accounts Opened by Identity Thieves, 2006**  
(Percent)



*Source:* This figure adapted from FTC 2006 Identity Theft Survey Report.

*Note:* Only the top 5 account types are presented.

Across all sectors, security experts cited identity theft as a serious threat to their businesses and customers. Credit cards, particularly store-issued cards, frequency cards,<sup>7</sup> and debit cards are extremely susceptible to identity theft and fraud. Experts cited improper storage of Track 2 data<sup>8</sup> as being the source of several recent large-scale data breaches, and maintained that storage problems will continue to pose problems across a variety of business sectors. Many merchants, whether intentionally or unknowingly, improperly store Track 2 data, making companies vulnerable to data breaches and increasing the opportunity for identity theft. Improper retention of identifiable or sensitive data, whether it is customer information from a debit card purchase or an employee's personal and financial information, puts both the company and individual at risk.

The retail industry is particularly vulnerable to identity theft because of the type and amount of data collected through various transactions. In addition, some merchants and credit card processing companies use antiquated database systems. These systems were designed long before today's security issues could have been anticipated, creating prime opportunities for fraud. Numerous data breaches have exposed these vulnerabilities and as a result, Payment Card Industry (PCI)<sup>9</sup> standards were created to prohibit retailers from storing Track 2 data and PINs.

<sup>7</sup> Frequency cards (also known as reward cards) are plastic cards with a magnetic strip containing information that tracks the use or purchase of a product or service in order to offer a prize or discount for reaching a particular goal. These cards are often used by retail and services industries to encourage loyalty to their food, products, or services.

<sup>8</sup> Track data refers to the information encoded in Track 1 and 2, within the magnetic strip on the back of a debit- or credit-card, which is read by a merchant's point-of-sale (POS) system. Track 2 data includes account numbers, security codes, and expiration dates.

<sup>9</sup> The PCI Security Standards Council was formed by American Express, Discover Financial Services, JCB, MasterCard Worldwide, and Visa International to enhance data security by adoption of agreed upon standards concerning cardholder data. The core principles of PCI Standards are to: build and maintain a secure network; protect cardholder data; maintain a vulnerability management program; implement strong access control measures; regularly monitor and test networks; and maintain an information security policy.

<https://www.pcisecuritystandards.org/>

Several states enacted data storage legislation (e.g., the Minnesota Plastic Card Security Act<sup>10</sup>). Unfortunately, compliance with PCI standards is uneven at best (large and middle-sized merchants are more likely to be compliant than are smaller merchants), and relatively few jurisdictions have enacted state-specific legislation. Security experts predicted that it would take a large-scale publicly disseminated data breach for national legislation to be enacted.

Other industries are also vulnerable to identity theft. For example, health care security experts noted that the large numbers of people entering and exiting hospitals and health care facilities on a daily basis generate a considerable amount of patient and employee information that can become vulnerable to theft. Medical identity theft occurs when a perpetrator uses another person's identity to obtain medical care, to sell that information to other people, or to file a false medical claim. In addition, health care security experts explained that in a hospital setting, security is often not at the forefront of patient or family member's thoughts, making them at risk for identity theft (as well as theft of personal belongings) when they leave valuables unattended or their vehicles unsecured.

Security experts from the banking and insurance sectors provided several examples of how and when identity theft or fraud might occur, including when employees do not properly secure laptops or when password protected desktop computers are not secured. Staff may also improperly discard personal information from credit applications when processing loans or credit approvals. In addition to these acts of negligence, employees may take an active role in identity theft, such as when call center employees retain clients' personal or identifiable information for the purpose of selling that information.

Security experts cited the theft of identities through "skimming" as an emerging problem. Skimming involves fraudulently obtaining credit or debit card information through the use of a small device (card reader) that can be attached to an automatic teller machine (ATM), credit card processing machines, and bill payment kiosks. In addition, portable card readers can be used to obtain information from stolen credit or bank cards. Once information has been stolen, it can be used to create counterfeit ATM cards, debit cards, credit cards, frequency cards, and gift cards.

While the various forms of identity theft referenced above have increased over time, security managers should not assume they would be ahead of the curve by simply responding to current identity theft methods. Rather, as the identity theft field matures over time, security experts should expect an increase in more organized, high-stakes, global attacks. This includes targeting high-profile corporate executives, for which much personal information is publicly available and can be used to access their financial holdings. Efforts to reduce these more sophisticated and wide-scale identity thefts will require coordination across international, federal, state, and local law enforcement agencies.

Unfortunately, many security experts feel such coordination is a lofty goal, even on the local level. Experts across all sectors observed that while efforts are underway to prevent identity theft (e.g., using multiple layers of authentication for online banking or retail shopping, and offering rewards for information leading to the arrest of individuals using skimming devices), local law

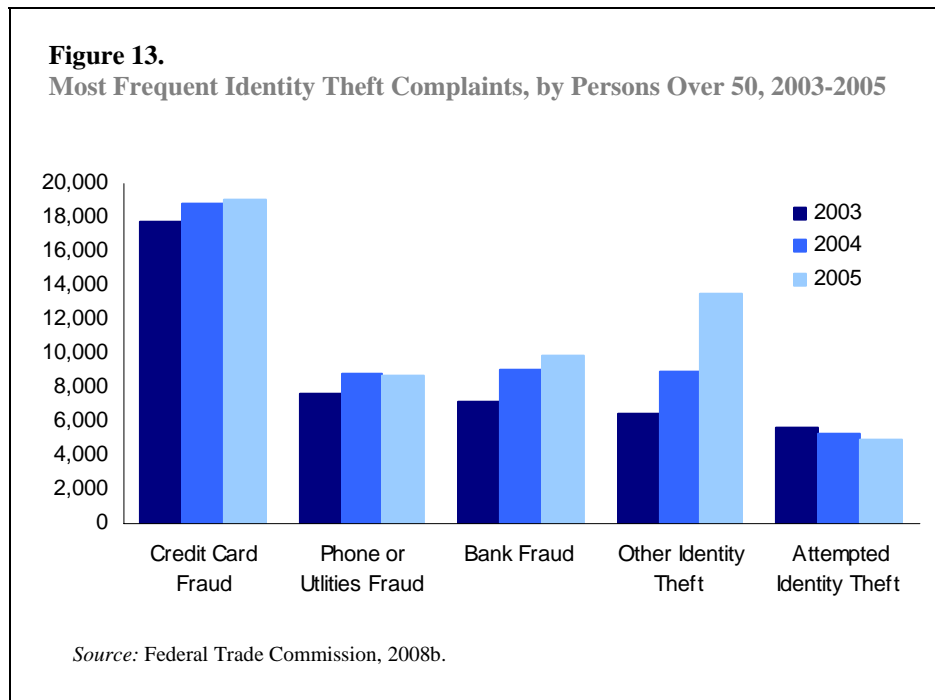
---

<sup>10</sup> The legislation prohibits companies or retailers from keeping secure information stored on a credit-or debit-card's magnetic strip in their computer databases after a transaction is completed. The magnetic strips on payment cards contain sensitive information such as the customer's name, account number, PIN, card expiration date, and security code data. [http://www.senate.leg.state.mn.us/members/member\\_pr\\_display.php?ls=0&id=925](http://www.senate.leg.state.mn.us/members/member_pr_display.php?ls=0&id=925)

enforcement is not well positioned to respond to these criminal complaints. Security experts cited ambiguity among some law enforcement agencies regarding jurisdictional responsibilities and the procedures governing reports and investigations of identity theft. In addition, victims are not always aware of the importance of filing a complaint with the local police department or the procedures for doing so. This lack of clarity of roles and responsibilities on the part of both victims and law enforcement can create the perception among offenders that identity theft is a crime with minimal risk of detection or punishment.

***Victimization***

All security experts agree that the victimization of older persons is an important security issue. The National Crime Victimization Survey revealed that persons aged 65 and older are disproportionately affected by property crimes with more than 90 percent of crimes against this group being property crime and more specifically, 20 percent cited as theft (Catalano 2006). According to experts, as older persons become consumers of personal technology products, such as cell phones and MP3 players, they will be at increased risk of victimization. Older Americans might also become more vulnerable due to the explosive growth in assisted living facilities, which will generate increased security needs, such as background checks of facility workers and standards and inspections of the facilities themselves, to prevent elder abuse.



We can expect that, as the population ages in the future, the elderly will increasingly be targeted for fraud and confidence scams. As shown in figure 13, overall, identity theft complaints by persons over the age of 50 increased between 2003 and 2005.

According to representatives from the banking, insurance, and information technology sectors, older persons are particularly vulnerable to identity theft and computer-related fraud. They noted that while older people will become more computer savvy in the future, they will also be using the computer more for online purchases and e-mail, making their personal information less

secure and making them more susceptible to phishing. Indeed, because older Americans tend to have more wealth accrued than their younger counterparts; they will make for more lucrative targets for fraud and theft. Efforts to educate older populations on ways of protecting themselves are important considerations for security managers.

### Recommendations:

- Use fraud detection systems and multiple layers of authentication, including validating Track 2 data in addition to PIN numbers
- Support legislation that addresses security of Track 2 data
- Use PINs in conjunction with frequency or gift cards and package them so card numbers are not visible
- Follow compliance regarding the storage of sensitive data
- Remove personal information from any place that may afford public access or be vulnerable to hacking; especially personal data on senior-level executives
- Provide local law enforcement with detailed information on preventing and responding to identity theft
- Encourage banking, insurance, and credit card companies to utilize smart cards<sup>11</sup>
- Improve hardware on ATM machines, bill payment kiosks, and credit card processors to make them less vulnerable to tampering/skimming
- Collaborate across merchants, industries, and organizations to identify and address security breaches and crime trends
- Encourage senior citizens to shred everything that has personal information. Alert them to the Web site, [www.onguardonline.gov](http://www.onguardonline.gov), which provides detailed information on computer security and Internet fraud

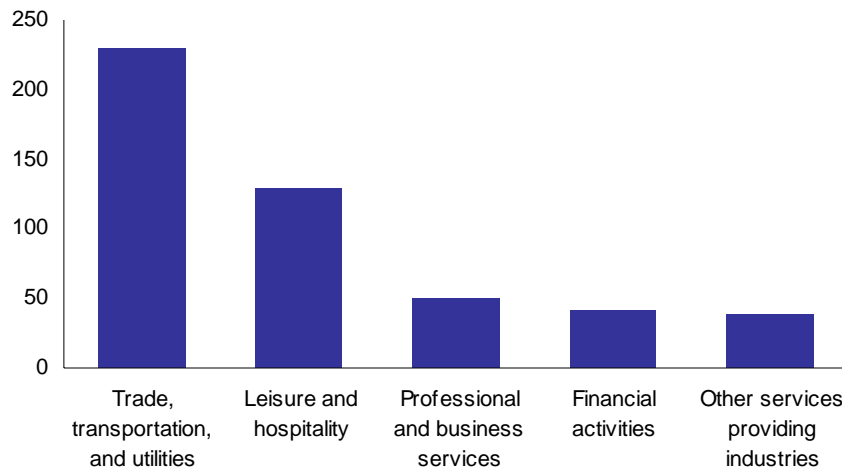
## Workplace Violence

Each year approximately two million workers are victims of violence (OSHA 2002). In addition, 13 percent of all workplace fatalities result from assaults or violent acts (U.S. Department of Labor 2007). As figure 14 illustrates, workplace violence affects every major industry sector. Some workers, by the very nature of their jobs, are more vulnerable to acts of violence than others, such as those who exchange money with the public; deliver passengers or goods; work alone or in small groups; work late night or early morning hours; work in high-crime areas; and work in community settings, such as hospitals, institutions, and group homes (OSHA 2002). In addition, four out of 10 robbery victims were victimized while working in retail sales or in the transportation industry (Duhart 2001).

---

<sup>11</sup> A device embedded with a microchip that contains information that connects to a reader through direct contact or through remote contactless radio frequency (Smart Card Alliance 2008).

**Figure 14.**  
**Fatal Occupational Assaults and Violent Acts, by Major Industry Sector, 2006**  
 (Number of injuries)



*Source:* U.S. Department of Labor, Bureau of Labor Statistics, in cooperation with State and Federal agencies, Census of Fatal Occupational Injuries, 2006

*Note:* Only the top five major industry sectors are presented.

While workplace violence overall has declined in recent years, the number of victimizations remains high and security experts predict an upswing in the coming decade. Indeed, with the exception of the information technology sector, most security experts expressed concern that violence in the workplace is on the rise and that people are more likely to resort to violence during a conflict today than in the recent past. Security experts from the hospitality and health care industries were the most likely to predict an increase in workplace violence, noting that domestic violence, gang activity, and acts of retaliation are increasingly brought into the workplace. Some security experts posit that the increases in workplace violence are emblematic of society's desensitization to violence. Retail security experts observed that many of the physical altercations occurring in their businesses are the result of clashes between people of differing cultures, nationalities, ethnicities, and beliefs. Health care, retail, and hospitality security experts also noted that the nature of their businesses is to be open to the general public, making them particularly vulnerable to violence and restricting security options because open access is intrinsic to their business. Security experts from the health care sector said their environments are exceptionally volatile because patients and family members are often under a high degree of stress. This is particularly true in the case of gang members who enter the hospital as patients. More often than not, when gang members are admitted for a gunshot or knife wound, gang issues follow them into the hospital.

In addition to workplace violence, banking, insurance, and hospitality security experts expressed concern with an anticipated increase in robberies. These concerns were offset by the observation that smaller amounts of money are being taken than in years past. They attributed this decrease to improved cash handling procedures, better security training, and the increased use of technology, such as software programs and hardware devices. While these advances are promising, some security experts cautioned that offenders will adapt to new technologies and that effective crime prevention requires constant vigilance and continued innovation.

## Recommendations:

- Provide employees with information on victims' rights and where to get help
- Employ improved cash handling procedures, encourage the use of drop boxes, and take advantage of new technologies to reduce the amount of cash lost in robberies
- Provide employees with training to recognize and address conflicts in an appropriate manner and to be aware of behaviors that might escalate into violence
- Offer cultural awareness training and encourage tolerance among employees
- Provide employees with access to substance abuse and mental health services or counseling

## Organized Retail Crime

Of the crime trends on the horizon, perhaps the greatest threat to future security managers, particularly those in the retail sector, is Organized Retail Crime (ORC). Also known as organized retail theft, ORC is the theft of merchandise, usually in large quantities, from retailers in which groups of people collaborate to steal and then resell stolen merchandise (National Retail Federation 2007). Thefts commonly occur from understaffed, minimally secured, and crowded stores, warehouses, and trucks (Pressler 2005). Items at greatest risk of ORC include: health and beauty products, over-the-counter drugs, baby formula, pain medication, gift cards, electronics, luxury clothing, and accessories (Hill 2007; Earnest 2008). Organized groups use a range of methods to steal items, such as changing the UPC codes to ring up as a lower price, working in teams to boost<sup>12</sup> items, or using stolen or counterfeit cards to make purchases (Hill 2007). Stolen goods are resold through fencing<sup>13</sup> operations at flea markets, pawn shops, on street corners, online auction sites, or even at other stores. ORC accounts for an estimated loss of \$30 to \$37 billion dollars per year (FBI 2007). In addition, profits from some ORC theft rings are thought to fund terrorist activities (Emerson 2005).

The National Retail Federation (NRF) reported that 79 percent of retailers were victims of ORC within the past year and that many retailers have observed an increase in ORC activity within the past 12 months (NRF 2007). The Internet has fueled the growth of ORC by providing access to a global customer base, an unregulated arena, and anonymity (Hill 2007; Brekke 2007; Earnest 2008). It can also be more lucrative; online fencing operations can bring in 70 cents on the dollar, whereas physical fencing operations pay around 30 cents on the dollar (Hill 2007). In addition, street gangs typically involved in illegal drug sales have gravitated toward ORC because it is seen as a lucrative, low-risk business (Earnest 2008).

Among the anticipated crime problems cited by security experts, the problem of ORC emerged prominently, particularly among retail experts, who fear multi-billion dollar losses. According to retail experts, the effect of ORC will extend beyond corporate financial losses, impacting local economies through the loss of sales tax revenue, and ultimately affecting consumers when losses

---

<sup>12</sup> Boosters are thieves who work in teams of two to steal items. One thief will distract a store employee while the other takes items from shelves or a supply room.

<sup>13</sup> Fencing refers to selling stolen goods for resale purposes.

are passed along in the form of higher prices. In addition, ORC has the potential to put public health and safety at risk. For example, infant formula, a common target of retail theft, may not be stored properly before resale, causing it to spoil and become a serious health risk for infants.

According to security experts, ORC will continue to flourish, specifically through online fencing. Due to the ease of use and relative anonymity, online sales through outlets such as auction sites and community postings provide an ideal black market for stolen merchandise. Indeed, security experts observed that the Internet has enabled professional thieves to operate within the global marketplace in the same manner as legitimate businesses.

Security experts noted that ORC is further complicated by a lack of cohesive law enforcement involvement, particularly among local law enforcement agencies. Retail security experts expressed concerns that local police departments are not well versed in the nature of the problem and have a limited ability to respond to and investigate cases. Some experts believe ORC is not a priority for local law enforcement because it is viewed as “just another shoplifting case.” One security expert remarked that when one of his stores called the police to report these crimes the officer cautioned store management that they were reporting too many thefts and that they would be charged with disturbing the peace if they continued. While a simple theft might appear as a single isolated incident, retail security experts posited that if these incidents were fully investigated, a pattern of criminal activity related to organized crime may well be revealed.

In April 2007, retail industry organizations and the FBI launched the Law Enforcement Retail Partnership Network (LERPnet),<sup>14</sup> a Web-based database that allows retailers to share information relating to ORC and major criminal incidents with each other and with law enforcement. Created in partnership with the FBI, National Retail Federation, and Retail Industry Leaders Association, LERPnet is currently used by 65 retailers representing more than 85,000 stores nationwide. More than 25,000 incidents have already been reported. In time, the system will allow users to learn more about what states, stores, and merchandise are most at risk.

### **Recommendations:**

- Use the Law Enforcement Retail Partnership Network (LERPnet)
- Collaborate with local law enforcement to develop reporting protocols for ORC activities
- Provide employees with training to identify behaviors and situations associated with ORC. Reward staff for reporting incidents of theft and suspected ORC
- Collaborate with product developers to design potential hot products in a way that minimizes vulnerability for theft
- Urge lawmakers to enact laws that address all aspects of ORC, including enhanced penalties

---

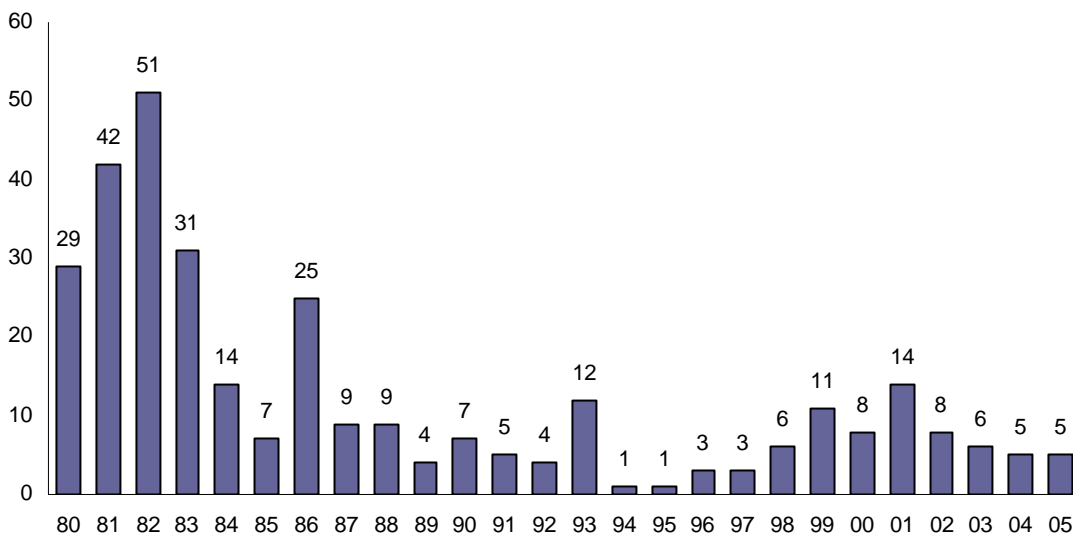
<sup>14</sup> LERPnet is a secure database for reporting retail theft and serious incidents. LERPnet is the result of a partnership between the FBI and the retail industry for the purpose of sharing information with other retailers and law enforcement. LERPnet is expected to be the standard for sharing retail crime information. <http://www.lerpnet.com>

## Terrorism

Since 1980, the number of terrorist incidents in the United States has fluctuated, but the overall trend indicates a decline in incidents over time (figure 15). This trend, however, does not represent the seriousness of terrorist events in terms of fatalities and damage to major infrastructure.

The majority of security experts across business sectors cited terrorism as a concern; transportation experts in particular noted that the threat of terrorism, specifically a catastrophic attack with mass casualties, as their most pressing security issue. Nonetheless, these experts voiced concerns that increased scrutiny over potential terrorist incidents has led to a greater number of unfounded incidents and false security breaches, which can drain resources. Furthermore, some security experts expressed concern that the current approach to investigate any and every suspicious incident (regardless of its relationship to a terrorist threat) makes organizations more vulnerable to future attacks. For example, when an organization responds to every incident, observant criminals could easily gather intelligence about how the industry will respond to potential breaches or “distractions” and amend their strategies accordingly.

**Figure 15.**  
Terrorism Incidents, United States, 1980-2005  
(Number of incidents)



Source: This figure adapted from the *Federal Bureau of Investigation, Terrorism 2002-2005* report.

Security experts noted that while it is difficult to assess whether current security practices would have any effect in preventing future terrorist activities, one measure for effectiveness is the extent to which they have led to a decrease in other criminal activity. For example, security experts observed that strategies such as using K-9 patrols to sniff out explosives, requiring passengers to produce identification with their tickets, and increasing visibility of officers on patrol, have led to a decrease in quality of life crimes and drug trafficking. Moreover,

transportation security experts suggested that crime prevention strategies implemented to address a range of crimes and criminal behavior can help identify or disable potential terrorist activities. For example, banking and insurance security experts observed that terrorist groups might come to the attention of financial institutions when laundering money. This point emphasizes the importance of interagency coordination and increased communication across sectors, bringing together public agencies and private businesses to address crime and criminal behavior.

Another issue of concern, particularly for security experts from the retail and hospitality sectors, is the vulnerability of the agricultural infrastructure. Food security is a complex issue; from distribution to the pantry, food is a soft target and having a comprehensive plan in place involves collaboration across several industry sectors (U.S. Department of Health and Human Services 2006). Industries are very conscious of this risk; however, security experts are still challenged by the ease with which someone could tamper with products once they are on the shelf.

Security experts also anticipated an increase in terrorist acts on vulnerable soft targets such as shopping malls, hotels, and hospitals. This all too real threat calls for the increasing adoption of noninvasive screening and access control technology, such as CCTVs coupled with video analytics, metal and explosive detectors, and biometrics to increase security in public places.

However, as health care security experts observed, planning for a terrorist attack is as challenging and resource draining as planning for any type of catastrophic incident. In addition to screening and access control technologies, experts advocated for more training and mock attack exercises that are flexible enough to address a range of scenarios. For example, some participants remarked that even with significant attention and funding for Avian Flu preparedness programs, the reality is that the ability to respond to an outbreak is questionable. Overall, security experts believed that the health care industry has made strides to better prepare itself, such as developing regional emergency councils and communicating with their peers. Unfortunately, these preparedness efforts are challenged by the reality that an incident may surface in a way that was never anticipated.

### **Recommendations:**

- Increase visibility of security staff to deter criminal activity
- Approach terrorist prevention through the lens of crime prevention
- Implement security measures consistently (e.g., if identification is required at the ticket counter, comparable identification should be required at the ticket kiosk)
- Respond to security breaches and possible threats in a way that does not reveal security protocols
- Implement flexible and adaptable incident response management plans based on a variety of factors, including resource allocation and staffing

## Section 5

# TECHNOLOGY

Technology has changed the way we live—from the ways we do business to how we communicate with each other. People rely on technology to communicate through e-mail and cellular phones. The increased use of Bluetooth and Wi-Fi technology allows individuals to be more productive, efficient, and accessible. In addition, people opt to shop and conduct financial transactions online instead of in person. Rather than using cash or checks, consumers are increasingly using credit and debit cards to make purchases or withdraw cash. Smart cards equipped with microchips are used to access buildings and for public transportation purposes. Medical, financial, personnel, and operating information and records are now stored in large databases through complex networks and information systems. These technologies have changed the landscape of how security professionals perform their duties. As described through the perspectives of security experts below, some aspects of technology enhance security and increase efficiency and productivity in the workplace, while others pose threats. The use of the Internet, reduced human interaction, proliferation of information systems, and portability of electronics will likely lead to increased opportunities for crime.

## Using Technology Creates Opportunities for Crime

### *Internet Use*

The United States has the highest saturation of Internet use; however, the Web is a global tool and the growth rate of Internet use in other areas around the world is significant (Internet World Stats<sup>14</sup> 2007). From 2000 to 2007, the largest amount of growth in Internet use was in the Middle East (920 percent) and Africa (882 percent). During that same period, Internet use in North America increased 120 percent (Internet World Stats 2007). As shown in Table 16, younger people in America, those under the age of 29, are more likely to use the Internet for social activities such as instant messaging than older adults. Experts from the Pew Internet and American Life Project found blogging and playing online games to also be among the top Internet activities for younger people (Fox 2005). Adults, on the other hand, are more likely to use the Internet for activities that require capital, such as online banking (Madden 2006).

Society has become increasingly dependent on the Internet to perform a variety of tasks as well as to provide a source of entertainment (Madden 2006), thus creating new opportunities for crime. The sheer volume of data accessible and transmitted via the Internet is almost immeasurable. Several security experts noted that the wealth of information available online, and the anonymity it provides, has contributed to the proliferation of crimes such as identity theft and fraud. Banking security experts identified phishing and pharming<sup>15</sup> activities as facilitators of crime. In addition, the use of online fencing resources such as “carder” chat rooms, where “data

---

<sup>14</sup> Internet World Stats (ISW) publishes usage and population statistics regarding the Internet. ISW compiles data from a variety of resources. Population data comes from the U.S. Census Bureau and usage data comes from Nielsen//NetRatings, Internet media and market research company. [www.internetworldstats.com](http://www.internetworldstats.com)

<sup>15</sup> Pharming misdirects users to fraudulent sites or proxy servers, typically through DNS hijacking or poisoning (Anti-Phishing Working Group, 2008).

thieves go to trade and sell access to eBay and PayPal accounts, hacked home computers, and airtime on Internet-based telephone networks,” are becoming more prevalent (Krebs 2005).

**Table 16.**  
**Online Activities, by Most Frequent Type and Generation, 2005**  
 (Percent)

Online Activity	All Online Adults <sup>a</sup>	Online Teens <sup>b</sup> (12-17)	Gen Y (18-28)	Gen X (29-40)	Trailing Boomers (41-50)	Leading Bloomers (51-59)	Matures (60-69)	After Work (70+)
<b>Go online</b>	<b>72</b>	<b>87</b>	<b>84</b>	<b>87</b>	<b>79</b>	<b>75</b>	<b>54</b>	<b>21</b>
Use email	91	89	88	92	90	94	90	89
Get health info on at least one topic	79	*	73	84	80	84	68	72
Product research	78	*	79	80	83	79	74	60
Get news	73	76	72	76	75	70	74	68
Online purchase	67	43	68	69	68	67	65	41
Travel reservations	63	*	50	72	64	64	59	60
School research	57	*	73	60	61	48	33	14
Use gov't sites	54	*	41	56	64	60	55	45
Job research	51	*	44	59	59	54	31	13
Instant message	47	75	66	52	38	42	33	25

Source: This figure adapted from Pew Data Memo, Generations Online, 2005.

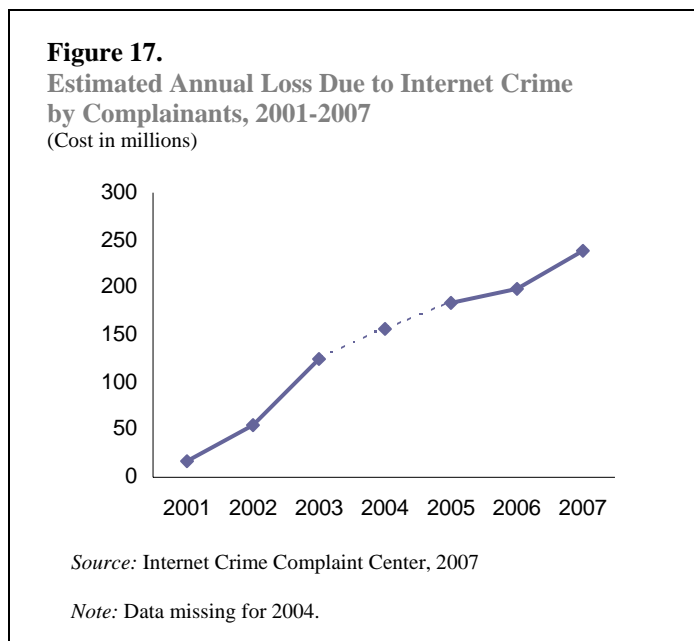
a Source: Pew Internet & American Life Project Surveys, January 2005, May-June 2005, and September 2005.

b Source: Pew Internet & American Life Project Teens and Parents Survey, Oct.-Nov. 2004.

In terms of anticipated crimes generated or facilitated by the Internet, security experts predict an increase in successful hacking attacks. As services such as online banking and BillPay become more commonplace, experts cautioned that the ability to hack into these accounts or use bank-stealing Trojans<sup>16</sup> to extract financial information and funds would increase. Thereby, the significant rise in financial losses reported by the Internet Crime Complaint Center<sup>17</sup> (IC3) (figure 17) is likely to continue its upward trend in the coming decade. In addition, the IC3 reports that almost half of the Internet crime victims were between the ages of 30 and 50, and that the amount of money lost increased with age (IC3 2008; Simmons 2008). Considering the increase in malicious online activity and the shift in demographics over the next 10 years, older persons, the group less likely to take precautions against such attacks, will be particularly vulnerable. (Fox 2006).

<sup>16</sup> A bank-stealing Trojan is malware (virus) that steals log-on information and funds from a financial account when a user clicks on a link, usually sent via e-mail, that downloads and installs a program onto the user's computer; waits for the user to log-on to their bank account, and then accesses that account (Evers 2006).

<sup>17</sup> IC3 is a partnership between the FBI, the National White Collar Crime Center, and the Bureau of Justice Assistance to receive, develop, and refer criminal complaints regarding cyber crime.



### ***Reduced Human Interaction***

Security experts posit that cybercrime will continue to rise in the coming decade. Many believe that increased Internet use will lead to reduced human interaction, removing an essential layer of protection against criminal behavior by making identification less verifiable, and increasing the opportunity for unauthorized access to information. Confidential data that was once locked away in a file room can be accessed today by hacking into a computer system. In addition to the increased ease of theft that the Internet affords, this lack of face-to-face contact makes it easier for criminals to justify or rationalize their offenses. Indeed, security experts argued that, for some offenders, crimes committed using technology, such as online transactions, are viewed as “victimless” and as not having any consequences or being particularly serious offenses. In essence, information technology desensitizes people to the culpability of engaging in certain types of criminal behaviors.

### ***Advancement of Information Systems***

Organizations are increasingly reliant upon information systems for operational purposes, and for most organizations, a compromised information system would be debilitating. Security experts predict that data breaches will become more common as companies continue to use expansive databases that are not properly protected. Security experts from the hospitality industry expressed concerns that they are increasingly at risk of such data breaches. Health care security experts observed that while technology has immensely aided their industry it also creates opportunities for data to be compromised. For example, a physician might forget to lock a computer screen, making confidential patient information available to unauthorized viewers. Similarly, as more physicians monitor patients and access medical records offsite, data will become increasingly vulnerable to security breaches. When discussing ways to prevent such vulnerabilities, security professionals cautioned against over reliance on technology and stressed the importance of keeping it simple, and implementing protocols that employ multiple layers of human review and interaction.

### ***Portability of Electronics***

According to the Pew Research Center, 62 percent of Americans use wireless, mobile technologies (Horrigan 2006). Security experts observed that as laptops, MP3 players, cell phones, PDAs, and USB devices become more commonplace, demand for such items would generate thefts. In addition, some researchers have argued that the increased use of portable electronic devices has caused a rise in violent crime (Roman and Chalfin 2007). As people become more mobile and communication technology becomes more advanced, portable devices will not only be in high demand for theft, but also as tools to commit crime. For example, laptops not only make data vulnerable (through, for example, the use of unsecured Wi-Fi), but are also a tool for criminals to operate their businesses and conduct illegal transactions.

## **Using Technology to Combat Crime**

While recent technology advances have created opportunities for crime, security experts indicated that technology has been—and will continue to be—a tremendous aid in security efforts. Security experts across all sectors offered examples of how software, surveillance technology, and information security counterintelligence<sup>18</sup> can increasingly be used to prevent and control crime.

### ***Surveillance***

Transportation security experts identified video surveillance as one of the most useful technologies for crime control purposes. They noted that while video surveillance can be a helpful investigative tool, its ultimate effectiveness is when it is actively monitored and records footage that can be retrieved at a later date. Similar to the transportation experts, banking and insurance security experts identified web-cameras as a promising crime prevention and detection technology for their industries. These cameras are commonly found on ATM machines or situated above register drawers and provide surveillance of financial transactions. Security experts argued strongly that these video technologies are most useful when integrated into a security plan with a human element, such as foot patrols, K-9 units, and crime analysts. They also cautioned that a move toward a more wholesale reliance on technology could engender a false sense of security, creating vulnerabilities for the industry, its employees, and the public.

### ***Software and Automated Security Devices***

From the perspective of retail security experts, the use of Radio Frequency Identification Device<sup>19</sup> (RFID) technology holds promise for improving crime control and prevention. RFID software, which works in concert with a RFID chip embedded in products, could be integrated with other systems to identify and measure the extent of internal shrinkage and shoplifting. Some

---

<sup>18</sup> Counterintelligence, typically associated with military tactics, refers to the use of data gathering activities to identify, and ultimately reduce, threats to a business, particularly with regard to its information system.

<sup>19</sup> RFID is a microchip that collects data and communicates that data with other devices. Together, the combination of chips, sensors, and software offer a range of capabilities but are typically used for inventory control for businesses or simple data collection. The software component of an RFID system offers considerable flexibility with regard to its capabilities. As the software advances, RFID applications will expand.

experts argued that current RFID applications are best used for measuring volume control, replenishing stock, or tracking merchandise, and that it would be too expensive to use RFID for both an operational and a crime prevention tool. With time, the cost of this technology is likely to decline, making it more accessible and encouraging use for a variety of security purposes.

Several industries currently benefit from security software that detects a threat or intrusion to their network or information system. Banking and insurance experts reported that anti-money laundering software and real time alerts are critical tools preventing crime in their industries. Financial institutions increasingly use anti-money laundering software, which issues alerts when transactions of certain dollar amounts or within certain time periods occur. Security experts predicted a greater reliance on this software in the future, and also cited an unmet need for other types of built-in and real-time alerts to identify suspicious account activity by both employees and external sources. This technology could aid in the detection of employee theft, which under current auditing mechanisms, is often not identified until after the offending employee has moved on to another job. However, customers may view it as overly intrusive and akin to profiling, leading them to potentially take their business elsewhere.

Health care security experts cited the benefits of automated security devices, from both an operational and a security (physical and network) standpoint. For example, automated medicine dispensers' help decrease pharmaceutical thefts. The automated machine dispenses and records medication for patients, and it requires the input of specific employee identifications and patient information for medicine to be dispensed. Security experts believed that these types of automated methods would become more commonplace in the future.

Experts from retail, banking, and insurance sectors also viewed video analytics, a software program used with video surveillance technology, as an emerging crime control tool. Video analytics software, while still in its infancy, analyzes specific behaviors, actions, people, objects, or data. Security experts viewed facial recognition software, a type of video analytics, as a particularly useful new technology to combat robberies. Surveillance cameras equipped with video analytics can identify suspicious behavior or known criminals when they come into view. Experts cautioned, however, that the storage of such video might create privacy concerns.

### *Counterintelligence*

Hospitality experts praised hacking conventions, such as DEFCON, as providing an excellent forum for security experts to gain intelligence on potential computer systems threats and to learn how to safeguard systems from attack. Typically open to the public, these conventions are attended by law enforcement and computer security professionals to gather intelligence on emerging computer and network vulnerabilities. Security experts stressed the importance of thinking like a criminal to catch a criminal. Another method of identifying network vulnerabilities and protecting information systems is with the use of a simulated network designed to detect attacks, capture worms and malware, and provide information on an attacker's methods, technologies, and motives (Bakos 2008). Termed a "honeypot" or "honeynet", this strategy can serve as an early detection system for possible intrusions and help security professionals identify attack vectors.

## Recommendations:

- Become familiar with other industries' security vulnerabilities and the technologies used to address them
- Invest in quality security software to detect and protect against risks to systems and employ strong encryption to protect sensitive data
- Train employees to understand how technology works, why it is being used, and how it is useful in creating a safe and secure working environment
- Educate the public as to how online activity might be supporting criminal operations (such as purchasing stolen goods through online auction sites)
- Incorporate a sound information security policy for employees, including one that addresses sensitive data on portable devices
- Implement policies for employee use of USB devices, restricting storage of sensitive data and the use of USB devices on work computers

## Section 6

# SPECIAL TOPICS

## Public Policy and the Law

The influence of public policy, including regulations and legal actions, was prominent in all roundtable discussions. Experts from all sectors faced difficulties complying with the vast number of regulations governing their industries. More specifically, the banking and insurance security experts stated that they are required to adhere to guidelines that are often difficult to implement. For example, security officers who are required to carry weapons must first undergo extensive security clearances. Yet background checks for the carrying of weapons are hindered by limited access to criminal history databases for state and federal agencies. Similarly, health care representatives discussed the Health Insurance Portability and Accountability Act's (HIPAA) regulations, which are strictly enforced by agencies such as the Joint Commission on Accreditation of Healthcare Organizations. While implemented with the best intentions, HIPAA requirements can impede investigations by restricting the release of information to law enforcement. For example, a security expert from the health care sector shared the story of how law enforcement officers were unable to obtain critical investigative information from a gunshot victim admitted to the emergency department. Other experts, particularly those in the transportation sector, shared that many policies and regulations are difficult to interpret and adhere to because regulatory language tends to lack specificity.

In addition, a common complaint across all sectors is that legislation tends to be reactive rather than proactive. As one information and technology security expert termed it, legislators have an "inertia problem," only passing new laws after catastrophic or publicly prominent events occur, such as the terrorist attacks of 9/11 or the corporate malfeasance leading to the passage of the Sarbanes-Oxley Act. Another participant noted that security is event-driven; prior to the attacks of 9/11, the security industry was scaling back and the next day executives were questioning why security departments were understaffed. The information and technology experts cited the presidential elections and Iraq war as examples of events that have driven policies affecting the security industry. Security experts predicted that this trend will continue, with enhanced criminal sanctions and tighter regulations being introduced only after increases in electronic and digital crime reach catastrophic levels. Given that it is impossible to predict what those events may be, they recommended taking a more proactive approach to influencing laws and regulations.

### Recommendations:

- Make compliance a collaborative effort within each industry and find ways for improvement
- Advocate for clearly defined legislation with an unambiguous purpose and measurable implementation standards
- Be proactive about crime prevention policy. Collaborate with legislators to create necessary policies for crime control

## Enlisting the Public in Security Efforts

Security experts agreed that across all issues and challenges, the public is an important and often untapped participant in safety and security efforts. While in some respects, enlisting private citizens in security efforts is becoming more difficult as the terrorist attacks of 9/11 become more distant in the public's collective memory, in other regards, the public is more accepting of security measures (e.g., retail's use of public surveillance cameras). According to representatives from the transportation sector, the public is not ready to accept the types of extensive security measures that are employed in other countries, such as Israel, where suicide bombers are real and daily threats. Security professionals in the United States are currently challenged to demonstrate to the public the relevance of security measures and to refute charges that those measures serve simply as "window dressing."

Security experts can sow the seeds of cooperation now by welcoming assistance from the public and clearly broadcasting the fact that they are an integral part of any security effort. Such involvement could be as simple as alerting personnel to an abandoned bag, or as extensive as serving as additional eyes and ears for prevention purposes. For example, hobbyists, such as railroad buffs and outdoorsmen, could be used for their expertise, aiding in the identification of suspicious or irregular activity along rail lines and within national parks. As one transportation security expert observed, human nature dictates a desire to be a part of the solution. Educating the public on the purpose of security measures and enlisting their support will increase their appreciation for and tolerance of such measures. This includes efforts to reduce identity theft, which are increasingly shifting both the responsibility and the monetary losses of such crimes onto the consumer.

### Recommendations:

- Engage the public in security matters by informing them of safety and security issues and strategies for resolving such matters. This process could involve the media on a broad scale, simply posting information on bulletin boards within public facilities, or asking for feedback from consumers
- Develop a community-based approach to security and crime prevention that allows the public to be involved in the decision-making process and implementation of security measures. Recruit community volunteers for security programs and awareness efforts
- Share responsibility with the consumer and make security a collaborative effort

## Section 7

# CONCLUSION

As this report illustrates, current shifts and predicted changes in demographic, crime, and technology trends will create both challenges and opportunities for security managers. While the actual events of the next decade are impossible to predict with any certainty, it is safe to assume that the increased diversity in age, race, ethnicity, and culture in our society will likely create tensions that will significantly impact security efforts. The charge for security managers is to anticipate and offset those tensions by renewing their focus on recruitment, retention, training, and communication.

Similarly, the role of technology features prominently in future trends for the industry. A double-edged sword, technology can open the doors to new types of criminal offenses and security breaches and it can also enhance efforts to make those doors as impenetrable as possible. In adequately preparing for the potential downside of new technological advances, security managers would benefit from increasing their counterintelligence and computer penetration prevention efforts, revisiting those vulnerabilities early and often.

This report was generated in the hope that the recommendations provided would help security managers get—and stay—ahead of the curve on emerging security threats. While we present several concrete methods towards doing so, the single most important and overriding tactic put forth is that of collaboration. Security managers stand to make the greatest gains in improving the quality of intelligence and increasing the effectiveness of their jobs through the sharing of information, and resources with each other, their law enforcement counterparts, and the public.

## ABOUT THE AUTHORS

### **Nancy G. La Vigne, Ph.D.**

*Senior Research Associate*

Dr. La Vigne has 18 years of experience in policy research on crime and justice issues and is a senior research associate at the Urban Institute, where she focuses on prisoner reentry, the evaluation of criminal justice programs and technologies, and the spatial analysis of crime and criminal behavior. She has published widely on crime and justice topics, including prisoner reentry, crime prevention strategies, and crime mapping.

Previously, Dr. La Vigne was the founding director of the Crime Mapping Research Center at the National Institute of Justice, the research, technology, and evaluation arm of the U.S. Department of Justice (DOJ), and later served as Special Assistant to the Assistant Attorney General for DOJ's Office of Justice Programs. She has held positions as research director for the Texas state sentencing commission, research fellow at the Police Executive Research Forum, and consultant to the National Council on Crime and Delinquency. Her research has appeared in a variety of scholarly journals including *Journal of Research in Crime and Delinquency*, *Journal of Offender Rehabilitation*, and *Journal of Contemporary Criminal Justice*.

### **Samantha S. Hetrick, M.S.**

*Research Associate*

Ms. Hetrick is a research associate at the Urban Institute, where she conducts research on school violence prevention, gang reduction programs, CCTV use in public spaces, preventing vehicle crime, and crime displacement. She is skilled in the manipulation and statistical analysis of crime data using various statistical packages. Currently, Ms. Hetrick is the project director for the School-Based Violence Prevention and Demonstration Program and the Evaluation of CCTV Use in Public Spaces. Before joining the research team at UI, Ms. Hetrick studied the psychology of sexual deviance and the ecology of crime, while pursuing a graduate degree in criminal justice from Northeastern University.

### **Tobi Palmer, M.S.W., M.S.**

*Research Associate*

Ms. Palmer has several years of experience in the field of social science and is a research associate in the Urban Institute's Justice Policy Center, where she is a project director for several program evaluations. Her projects encompass a range of topics including: public/private crime prevention partnerships, prisoner reentry, criminal justice applications of technology, and situational crime prevention. Prior to working at UI, Ms. Palmer worked for various research, direct service, and public policy organizations. Ms. Palmer holds graduate degrees from the University of Pennsylvania in Social Work and Criminology. In addition, she has specialized training in the field of International Migration: Human Trafficking of Women and Children.

## GLOSSARY

The following terminology and definitions were used in this report and in most cases, obtained from the specified location.

**Anti-Phishing Working Group (APWG)**—The global pan-industrial and law enforcement association focused on eliminating fraud and identity theft resulting from phishing, pharming and e-mail spoofing of all types. APWG is made up of over 3,000 members, 1,700 companies and agencies worldwide, nine of the top 10 U.S. banks, the top five U.S. ISPs, hundreds of technology vendors, and national and provincial law enforcement worldwide.

**Automated Teller Machine (ATM)** —Also referred to as an automatic teller machine; an unattended electronic machine, typically found in a public place or outside a bank, for dispensing money and conducting other banking services.

**Avian Flu**—Usually refers to influenza viruses found chiefly in birds, but infections can occur in humans. <http://www.cdc.gov/flu/avian/>

**Behavioral Profiling**—Similar to racial profiling; to draw or characterize a person’s distinct demeanor based on the actions or activities of that person; typically used for identification of suspicious or criminal behavior.

**Burglary**—Also referred to as breaking and entering; the unlawful entry of a structure to commit a felony or a theft. Attempted forcible entry is included. [http://www.fbi.gov/ucr/05cius/about/offense\\_definitions.html](http://www.fbi.gov/ucr/05cius/about/offense_definitions.html)

**CCTV**—Closed-circuit television; a video surveillance system for which images from a camera are relayed to a monitor or other device (such as a video cassette recorder [VCR] or television [TV]) through wiring rather than broadcast through the air. <http://www.popcenter.org/library-glossary.htm>

**Confidence Scam**—Also referred to as “confidence game;” false representation to obtain money or any other thing of value, where deception is accomplished through the trust placed by the victim in the offender. <http://www.asisonline.org/library/glossary/c.pdf>

**Counterfeiting**—The manufacture or attempted manufacture of a copy or imitation of a negotiable instrument with value set by convention or law, or the possession of such a copy without authorization, with the intent to defraud by claiming the genuineness of the copy. For statutory purposes, counterfeiting is included within the definition of forgery. The chief distinction of counterfeiting is the prior existence of an officially issued item of value, which provides a model for the counterfeiter. Examples are currency, stamps, and bonds. In forgery, the model is absent. It is not a crime to possess a counterfeit item without knowledge or criminal intent. <http://www.asisonline.org/library/glossary/c.pdf>

**Cybercrime**—Unlawful or restricted activity on a computer, network, or the Internet.

**Embezzlement**—The unlawful misappropriation or misapplication by an offender to his/her own use or purpose of money, property, or some other thing of value entrusted to his/her care, custody, or control. [http://www.fbi.gov/ucr/05cius/about/offense\\_definitions.html](http://www.fbi.gov/ucr/05cius/about/offense_definitions.html)

**Fencing**—(1) Physical barrier installed to delineate a boundary or to deter, delay, or prevent unauthorized access to a protected area. <http://www.asisonline.org/library/glossary/f.pdf> (2) The act of receiving and selling stolen goods. <http://www.popcenter.org/library-glossary.htm>

**Fraud**—The intentional perversion of the truth for the purpose of inducing another person or other entity in reliance upon it to part with something of value or to surrender a legal right. Fraudulent conversion, obtaining of money or property by false pretenses, confidence games and bad checks, except forgeries and counterfeiting, are included. [http://www.fbi.gov/ucr/05cius/about/offense\\_definitions.html](http://www.fbi.gov/ucr/05cius/about/offense_definitions.html)

**Frequency Cards**—Reward cards that track the use or purchase of a product or service in order to offer a prize or discount for reaching a particular goal; often used by retail and services industries to encourage purchasing of merchandise or foods and brand loyalty.

**Health Insurance Portability and Accountability Act (HIPAA)** —A federal law requiring a national standard for electronic health care transactions and national identifiers for providers, health plans, and employers. It also addresses the security and privacy of health data. <http://www.cms.hhs.gov/hipaaGenInfo/>

**Identity Theft**—Identity theft occurs when someone uses your personally identifying information, like your name, social security number, or credit card number, without your permission, to commit fraud or other crimes. <http://www.ftc.gov/bcp/edu/microsites/idtheft/index.html>

**Internet**—A collection of networks, which includes the national, regional, and local networks, at a number of university and research institutions, military networks, and corporation-owned networks. The term “Internet” applies to this entire set of networks. All networks comprising the Internet are connected to each other. Users can send messages from any of them to any other, except where security or policy restrictions apply. <http://www.asisonline.org/library/glossary/i.pdf>

**Joint Commission on Accreditation of Health care Organizations (JCAHO)** —An independent, nonprofit organization that accredits and certifies more than 15,000 health care organizations and programs in the United States. <http://www.jointcommission.org/AboutUs/>

**Law Enforcement Retail Partnership Network (LERPnet)** —A secure national database developed by the retail industry and the FBI for the reporting of retail theft and serious incidents, which allows retailers to share information with each other and law enforcement. <http://www.lerpnet.com/>

**MP3 Player**—A portable digital audio player that stores, organizes, and plays audio files; MP3 stands for MPEG Layer-3 (Moving Picture Experts Group).

**Money Laundering**—The disguise of monetary proceeds to hide their true source, either from legal or illegal activities. The desire to do so is to move money, reduce its volume and change its character to allow for spending or investing, while sheltering it from detection and taxation. <http://www.asisonline.org/library/glossary/m.pdf>

**Organized Retail Crime (ORC)**—Also referred to as Organized Retail Theft; criminal activity involving theft of merchandise from retail establishments by persons who engage in crime as a primary source of income and who cooperate and coordinate illegal activity with one another. Organized retail crime often involves shoplifting, cargo theft, retail crime rings, and other organized crime. <http://www.asisonline.org/library/glossary/o.pdf>

**PCI Standards**—Also referred to as PCI Data Security Standards (DSS); a common set of industry tools and measurements to help ensure the safe handling of sensitive information. Initially created by aligning Visa's Account Information Security (AIS)/Cardholder Information Security (CISP) programs with MasterCard's Site Data Protection (SDP) program, the standard provides an actionable framework for developing a robust account data security process - including preventing, detecting, and reacting to security incidents. <https://www.pcisecuritystandards.org/>

**Pharming**—Similar to Phishing; a scam technique using false Web sites to attempt to steal personal information. <http://www.antiphishing.org/>

**Phishing**—attacks used to steal consumers' personal identity data and financial account credentials. Phishing attacks entail sending 'spoofed' e-mails to lead consumers to counterfeit Web sites designed to trick recipients into divulging financial data such as credit card numbers, account usernames, passwords, and social security numbers. Hijacking brand names of banks, e-retailers, and credit card companies, phishers often convince recipients to respond. Phishers also use Trojan spyware to steal information directly from a computer. <http://www.antiphishing.org/>

**Personal Identification Number (PIN)** —A number entered into and recognized by an automatic teller machine (ATM) or similar device when making a transaction. <http://www.asisonline.org/library/glossary/p.pdf>

**Racial Profiling**—Similar to behavioral profiling; to draw or characterize a person, using race as the primary determinant, typically used for identification of suspicious or criminal behavior.

**Radio Frequency Identification (RFID)** —A data collection system of a microchip attached to an item that communicates with other devices using radio waves. A device reader captures data and software then collects, organizes, and distributes the data. <http://www.microsoft.com/biztalk/en/us/wp-rfid.aspx>

**Robbery**—The taking or attempting to take anything of value from the care, custody, or control of a person or persons by force or threat of force or violence and/or by putting the victim in fear. [http://www.fbi.gov/ucr/05cius/about/offense\\_definitions.html](http://www.fbi.gov/ucr/05cius/about/offense_definitions.html)

**Sarbanes-Oxley Act of 2002**—Also referred to as SOX; legislation enacted to protect shareholders and the general public from accounting errors and fraudulent practices in the enterprise. The Sarbanes-Oxley Act of 2002, introduced changes to regulations applying to financial practice and corporate governance for public companies. The Act introduced new rules intended “to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws.”

*<http://www.smartcardalliance.org/pages/smart-cards-intro-glossary#S>*

**Skimming Devices**—Small and portable devices used to illegally record and store credit card account information. Skimming is the practice of obtaining information from a data storage device without the owner’s knowledge. Skimming is typically associated with magnetic stripe-based credit cards. *<http://www.smartcardalliance.org/pages/smart-cards-intro-glossary#S>*

**Smart Cards**—A device that includes an embedded integrated circuit that can be either a secure microcontroller or equivalent intelligence with internal memory or a memory chip alone. The card connects to a reader with direct physical contact or with a remote contactless radio frequency interface. With an embedded microcontroller, smart cards have the unique ability to store large amounts of data, carry out their own on-card functions (e.g., encryption and mutual authentication) and interact intelligently with a smart card reader. Smart card technology conforms to international standards (ISO/IEC 7816 and ISO/IEC 14443) and is available in a variety of form factors, including plastic cards, subscriber identification modules used in GSM mobile phones, and USB-based tokens.

*<http://www.smartcardalliance.org/pages/smart-cards-intro-glossary#S>*

**Soft Target**—An area or type of technology, such as networks and computers, vulnerable to being attacked, harmed, or weakened.

**Terrorism**—(1) The calculated use of violence or threat of violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological. (2) The unlawful use or threatened use of force or violence against individuals or property to coerce or intimidate governments or societies, often to achieve political, religious, or ideological objectives. *<http://www.asisonline.org/library/glossary/t.pdf>*

**Terrorist Attacks of 9/11**—A series of coordinated suicide attacks by foreign terrorists upon the United States that took place on September 11, 2001, resulting in approximately 3,000 deaths.

**Track Data**—The information, such as name or account number, encoded in the magnetic stripe of debit or credit cards, which is read by a merchant’s point-of-sale (POS) system.

**UCR**—In the United States, Uniform Crime Reports (UCR) is a nationwide, cooperative effort of more than 18,000 city, university and college, county, state, tribal, and federal law enforcement agencies voluntarily reporting data on crimes brought to their attention.

*[http://www.fbi.gov/ucr/cius2006/about/about\\_ocr.html](http://www.fbi.gov/ucr/cius2006/about/about_ocr.html)*

## REFERENCES

- Anti-Phishing Working Group. 2008. "Phishing Activity Trends Report."  
<http://www.antiphishing.org>
- Bakos, George. 2008. "Honeypots and the Enterprise: Intelligence-Based Risk Management."  
Institute for Security Technologies, Dartmouth College.  
<http://www.ists.dartmouth.edu/library/97.pdf>
- Brekke, Brad. 2007. "Testimony of Brad Brekke Vice President, Assets Protection, Target Corporation, before the House Judiciary Committee, Subcommittee on Crime, Terrorism, and Homeland Security, October 25, 2007."  
[http://www.losspreventionmagazine.com/archives\\_view.html?id=2037](http://www.losspreventionmagazine.com/archives_view.html?id=2037)
- Catalano, Shannan M. 2006. "Criminal Victimization, 2005." National Crime Victimization Survey. Bureau of Justice Statistics Bulletin. September 2006. U.S. Department of Justice.
- Curran, Kevin, Kevin Concannon and Sean Mc Keever. 2007. *Chapter I: Cyber Terrorism Attacks* in *Cyber warfare and Cyber Terrorism* eds. Lech J. Janczewski and Andrew M. Colarik. Information Science Reference.
- Day, Jennifer Cheeseman, Alex Janus and Jessica Davies. 2005. "Computer and Intranet use in the United States: 2003." *Current Population Reports, Special Studies*. U.S. Census Bureau.
- Duhart, Detis T. 2001. "Violence in the Workplace 1993-1999." National Crime Victimization Survey. Bureau of Justice Statistics Special Report. December 2001. U.S. Department of Justice.
- Earnest, Leslie. 2008. "Health Goods Sold on the Web Raise Concern." *Los Angeles Time*. Health section. February 20, 2008.  
<http://www.latimes.com/features/health/la-fi-tainted20feb20,1,1339649.story>
- Emerson, Steve. 2005. "Money Laundering and Terror Financing Issues in the Middle East. Testimony of Steve Emerson before the U.S. Senate Committee of Banking, Housing, and Urban Affairs." July 13, 2005.  
<http://www.investigativeproject.org/documents/testimony/19.pdf>
- Evers, Joris. 2006. "New Trojans Plunder Bank Accounts." CNET News.  
[http://www.news.com/New-Trojans-plunder-bank-accounts/2100-7349\\_3-6041173.html](http://www.news.com/New-Trojans-plunder-bank-accounts/2100-7349_3-6041173.html)
- Federal Bureau of Investigation. 2007. "Organized Retail Theft: New Initiative to Tackle the Problem." Archived Headlines from April 6, 2007.  
<http://www.fbi.gov/page2/april07/retail040607.htm>

- . “Terrorism 2002-2005.”  
[http://www.fbi.gov/publications/terror/terrorism2002\\_2005.pdf](http://www.fbi.gov/publications/terror/terrorism2002_2005.pdf)
- Federal Trade Commission. 2008a. FTC web site: About identity theft.  
<http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html>
- . 2008b. Consumer Sentinel web site: Consumer Sentinel fraud trends.  
<http://www.consumer.gov/sentinel/trends.htm>
- . 2007a. “Federal Trade Commission 2006 Identity Theft Survey Report.” Synovate.  
<http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf>
- . 2007b. “Consumer Fraud and Identity Theft Complaint Data, January–December 2006.” Data from Consumer Sentinel and the Identity Theft Data Clearinghouse. February 2007.  
<http://www.consumer.gov/sentinel/pubs/Top10Fraud2006.pdf>
- Federal Trade Commission. 2003. Consumer Sentinel website: Consumer Sentinel fraud trends.  
[http://www.consumer.gov/sentinel/states03/3year\\_trends.pdf](http://www.consumer.gov/sentinel/states03/3year_trends.pdf)
- Fox, Susannah. 2006. “Are ‘wired seniors’ sitting ducks?” Pew Internet & American Life Project. [http://www.pewinternet.org/pdfs/PIP\\_Wired\\_Senior\\_2006\\_Memo.pdf](http://www.pewinternet.org/pdfs/PIP_Wired_Senior_2006_Memo.pdf)
- Fox, Susannah and Mary Madden. 2005. “Generations Online.” Pew Internet & American Life Project. [http://www.pewinternet.org/pdfs/PIP\\_Generations\\_Memo.pdf](http://www.pewinternet.org/pdfs/PIP_Generations_Memo.pdf)
- Hill, David. 2007. “Testimony of Detective David Hill of the Montgomery County, Maryland Police Department on behalf of Law Enforcement Before the Subcommittee on Crime, Terrorism and Homeland Security of the United States House Committee on the Judiciary, October 25, 2007.”  
<http://judiciary.house.gov/hearings/pdf/1025073.pdf>
- Hoar, Sean B. 2001. “Identity Theft: The Crime of the New Millennium.” U.S. Department of Justice, Executive Office for United States Attorneys, *United States Attorneys’ USA Bulletin* 49(2): 1-10. [http://www.usdoj.gov/criminal/cybercrime/usamarch2001\\_3.htm](http://www.usdoj.gov/criminal/cybercrime/usamarch2001_3.htm)
- Horrigan, John. 2006. “Mobile Access to Data and Information.” Pew Internet & American Life Project. [http://pewinternet.org/pdfs/PIP\\_Mobile.Data.Access.pdf](http://pewinternet.org/pdfs/PIP_Mobile.Data.Access.pdf)
- Internet Crime Complaint Center. 2007. “Internet Crime Report 2007.” Internet Crime Complaint Center. National White Collar Crime Center, Bureau of Justice Assistance, Federal Bureau of Investigation.  
[http://www.ic3.gov/media/annualreport/2007\\_IC3Report.pdf](http://www.ic3.gov/media/annualreport/2007_IC3Report.pdf)
- Internet World Stats. 2007. IWS web site: Internet usage statistics. [www.internetworldstats.com](http://www.internetworldstats.com)

- Krebs, Brian. 2005. "Technology Fueling Wave of Phishing Scams." Washingtonpost.com. Technology section. January 18, 2005.  
<http://www.washingtonpost.com/ac2/wp-dyn/A17680-2005Jan18>
- Lenhart, Amanda, Mary Madden and Paul Hitlin. 2005. "Teens and Technology." Pre Internet & American Life Project.  
[http://www.pewinternet.org/pdfs/PIP\\_Teens\\_Tech\\_July2005web.pdf](http://www.pewinternet.org/pdfs/PIP_Teens_Tech_July2005web.pdf)
- Madden, Mary. 2006. "Internet Penetration and Impact." Pew Internet & American Life Project.  
[http://www.pewinternet.org/PPF/r/182/report\\_display.asp](http://www.pewinternet.org/PPF/r/182/report_display.asp)
- Mermin, Gordon, B.T., Richard W. Johnson and Eric J. Toder. 2008. "Will Employers Want Aging Boomers?" Retirement Policy Discussion Paper Series. Urban Institute.
- National Intelligence Council (NIC). 2007. "National Intelligence Estimate. The Terrorist Threat to U.S. Homeland. July 2007." [http://www.dni.gov/press\\_releases/20070717\\_release.pdf](http://www.dni.gov/press_releases/20070717_release.pdf)
- National Retail Federation (NRF). 2007. "2007 Organized Retail Crime Survey."  
[http://www.nrf.com/modules.php?name=News&op=viewlive&sp\\_id=305](http://www.nrf.com/modules.php?name=News&op=viewlive&sp_id=305)
- Occupational Safety and Health Administration (OSHA). 2002. "Workplace Violence. OSHA Fact Sheet." U.S. Department of Labor.  
[http://www.osha.gov/OshDoc/data\\_General\\_Facts/factsheet-workplace-violence.pdf](http://www.osha.gov/OshDoc/data_General_Facts/factsheet-workplace-violence.pdf)
- Pressler, Margret Webb. 2005. "Retail Gangs: A New Breed of Thieves." *The Washington Post*. July 31, 2005.  
<http://www.washingtonpost.com/wpdyn/content/article/2005/07/30/AR2005073001434.html>
- Roman, John and Aaron Chalfin. 2007. "Is There an iCrime Wave?" Research brief. September 2001. Urban Institute.
- Rugala, Eugene A. and Arnold R. Isaacs. 2004. "Workplace Violence: Issues in Response." National Center for the Analysis of Violent Crime, Critical Incident Response Group. U.S. Department of Justice, Federal Bureau of Investigation.
- Shin, Hyon and Rosalind Bruno. 2003. "Language Use and the English-Speaking Ability: 2000." Census Brief 2000. U.S. Department of Commerce. Economic and Statistics Administration. U.S. Census Bureau. October 2003.
- Simmons, Christine. 2008. "Internet Scams Cost Consumers \$240M." Associated Press. *Mercury News*. <http://www.mercurynews.com/topic/837Business/articles/73170380>
- Smart Card Alliance. 2008. SCA website: Smart card industry dictionary.  
<http://www.smartcardalliance.org/>

- U.S. Census Bureau. March 1997. "How We're Changing, Demographic State of the Nation: 1997." *Current Population Reports, Special Studies: Series P23-193*.
- U.S. Census Bureau. Population Projections Branch. "U.S. Interim Projections by Age, Sex, Race, and Hispanic Origin, 2004." <http://www.census.gov/population/www/projections/usinterimproj/>
- U.S. Department of Health and Human Services. 2006. "Terrorism and the Food Supply." <http://www.hhs.gov/disasters/press/newsroom/mediaguide/06.pdf>
- U.S. Department of Justice. 2008a. Fraud section: Identity theft and identity fraud. <http://www.usdoj.gov/criminal/fraud/websites/idtheft.html>
- . 2008b. UCR section: Uniform Crime Reports, 2000-2007. Federal Bureau of Investigation. <http://www.fbi.gov/ucr/ucr.htm>
- U.S. Department of Labor. 2007a. "Census of Fatal Occupational Injuries (CFOI) 2006." Bureau of Labor Statistics. <http://www.bls.gov/iif/oshwc/cfoi/cfch0005.pdf>
- . 2007b. BLS Employment Projections section: Employment by Major Industry, 2004, 2014. Bureau of Labor Statistics. <http://www.bls.gov/emp/#tables>
- . 2008a. "Foreign-Born Workers: Labor Force Characteristics in 2007." Bureau of Labor Statistics. <http://www.bls.gov/news.release/pdf/forbrn.pdf>
- . 2008b. "Labor Force Participation Rates, 2006-2016." Bureau of Labor Statistics. <http://www.bls.gov/emp/emplab1.htm>
- Wilson, Clay. 2008. "Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress." CRS Report for Congress. Congressional Research Service.



## ASIS International

ASIS International (ASIS) is the preeminent organization for security professionals, with more than 36,000 members worldwide. Founded in 1955, ASIS is dedicated to increasing the effectiveness and productivity of security professionals by developing educational programs and materials that address broad security interests, such as the ASIS Annual Seminar and Exhibits, as well as specific security topics. ASIS also advocates the role and value of the security management profession to business, the media, governmental entities, and the general public. By providing members and the security community with access to a full range of programs and services, and by publishing the industry's number one magazine, *Security Management*, ASIS leads the way for advanced and improved security performance. For more information, visit [www.asisonline.org](http://www.asisonline.org)



## ASIS Foundation

The ASIS Foundation, a 501(c)(3) charitable organization, provides funding and manages endowments for a wide range of academic, strategic, and professional development activities. The purpose of the Foundation is to enhance the security profession worldwide by establishing, developing, delivering, and promoting programs that advance security through education, research, and training. The Foundation, through the awarding of scholarships, ensures that those pursuing a career in security management are able to realize the highest academic achievements. Support for the Foundation is achieved through financial contributions from individuals, chapters, and companies employing ASIS members, and corporations with an interest in security. For more information, visit [www.asisfoundation.org](http://www.asisfoundation.org)

## The Urban Institute

The Urban Institute is a nonprofit, nonpartisan policy research and educational organization established in Washington, D.C., in 1968. Its staff investigates the social, economic, and governance problems confronting the nation and evaluates the public and private means to alleviate them. The Institute disseminates its research findings through publications, its web site, the media, seminars, and forums.

The Urban Institute's Justice Policy Center carries out research to inform the national dialogue on crime, justice, and community safety. Its researchers collaborate with practitioners, public officials, and local organizations to make the Center's research useful to decision makers and agencies in the justice system and to the neighborhoods and communities harmed by crime and disorder.

