ASIS FOUNDATION

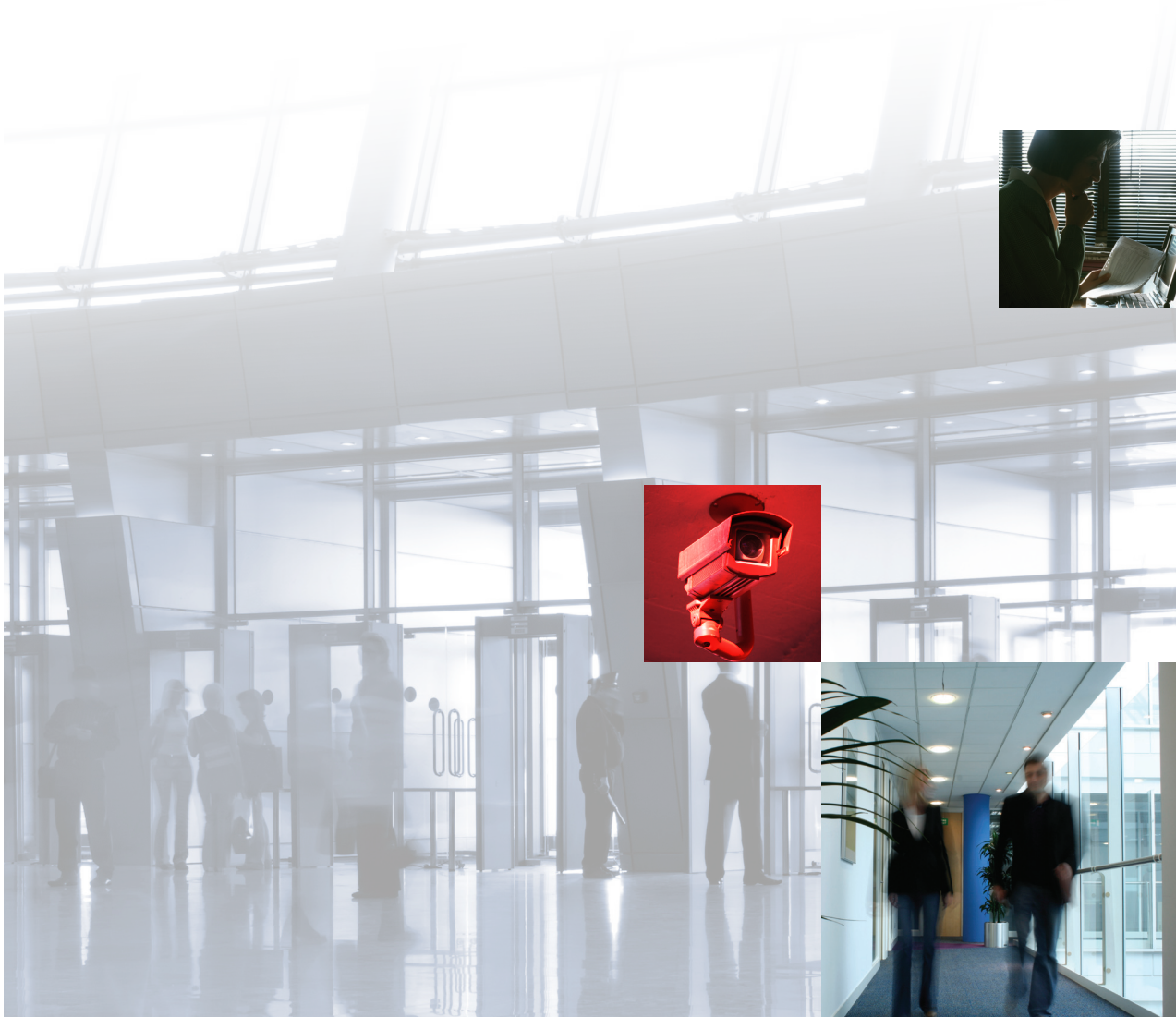
ASIS FOUNDATION™

CRISP REPORT

Connecting Research in Security to Practice

Tackling the Insider Threat

Nick Catrantzos, CPP



ABOUT THE CRISP SERIES OF REPORTS

Connecting Research in Security to Practice (CRISP) reports provide insights into how different types of security issues can be effectively tackled. Drawing on research and evidence from around the world, each report summarizes the prevailing knowledge about a specific aspect of security, and then recommends proven approaches to counter the threat. Connecting scientific research with existing security actions helps form good practices.

Reports are written to appeal to security practitioners in different types of organizations and at different levels. Readers will inevitably adapt what is presented to meet their own requirements. They will also consider how they can integrate the recommended actions with existing or planned programs in their organizations.

This CRISP report focuses on managing the insider threat. In addition to evaluating traditional approaches, the author Nick Catrantzos, CPP, reports on new research which posits a different way of dealing with the potential threat posed by those who work in the organisation. His insights align with those who advocate the importance of a positive security culture, as he supports a greater role for engaging staff meaningfully in the protection of the organisation. His approach, termed 'no dark corners' draws upon a range of others that will be familiar to many readers, and his findings will invite many to critically assess whether they are doing all they can, in the best way, to manage different types of insider threat.

CRISP reports are sister publications to those produced by Community Oriented Policing Services (COPS) of the U.S. Department of Justice, which can be accessed at *www.cops.usdoj.gov.* While that series focuses on policing, this one focuses on security.

Martin Gill
Chair, Research Council
ASIS Foundation

ISBN-978-1-934904-06-0

Printed in the United States of America

CRISP REPORT

Connecting Research in Security to Practice

An ASIS Foundation Research Council CRISP Report

Tackling the Insider Threat

Nick Catrantzos, CPP

ASIS Foundation, Inc. : Alexandria, VA

Contents

Executive Summary

All a hostile insider needs to carry out an attack are access to a worthy target, an open door, and a dark corner from which to study and strike. Insider threat studies abound, and the malicious insider phenomenon remains statistically rare yet potentially devastating to any institution with critical assets to defend. Accepted wisdom offers conventional security advice: preemployment background investigations, random audits, tighter access controls, more invasive monitoring through procedural or technological innovations.

This report combines a review of the insider threat literature with the findings of a Delphi study to arrive at a new approach to defeating the kind of trust betrayer intent on carrying out an attack that is fatal to the organization. While the Delphi research itself began with substantially the same views and counsel as prevailing wisdom represented in the literature, it ended altogether somewhere else. Certain pivot points in the research revealed that a reasonably prepared infiltrator poses a greater threat than a disgruntled career employee—at least if the focus is on adversaries bent on bringing an institution to its knees, rather than on exacting revenge against bosses or carrying out nuisance-level attacks against the employer.

Research findings also highlighted flaws in traditional defenses, including background investigations that identify neither the prepared infiltrator nor the future disgruntled careerist. Findings even suggested random audits are seldom truly random and pose only a surmountable hurdle to a worthy adversary. Moreover, ineffective exercise of employer prerogatives like probationary periods appears underexploited as an insider threat defense.

Into this context, a new approach emerged. This approach is about engaging co-workers on the team level to take a hand in their own protection. It calls into protective service the vast majority of employees consigned to the sidelines and sometimes referred to as the weakest link in insider defense. Instead, with a shift in emphasis toward more productive countermeasures, the proposed alternative brings these people off the sidelines and onto the front lines, making them the first line of defense.

No Dark Corners extends to private spaces and institutions the seminal theories of proprietary interest and ownership that "Defensible Space" and "Fixing Broken Windows" demonstrated for public housing and community environments. In defending against insider threats, this approach proposes less emphasis on the laser of specialized monitoring by corporate sentinels. Instead, it promotes using the flashlight of open team engagement as a method of implementing layered defenses, particularly on the front lines of detection and intervention, where critical operations take place.

Introduction

Frontal attacks can be anticipated or met with traditional fortifications whose effectiveness is limited only by resources and imagination. However, attackers operating from within need not concern themselves with amassing superior force to breach fortified targets. Instead, hostile insiders can carry out attacks that are fatal to an organization without requiring an opposing army or sophisticated weaponry. Given sufficient access and maneuvering room, trust betrayers can be devastating. This we know, because insider threats repeatedly surface as an abiding concern for defenders. Nevertheless, insider threats remain statistically rare, making them harder to analyze, defend against, or anticipate.

What do we do about insider threats? Prevailing wisdom recommends doing more: look harder, submit ourselves to newer and more microscopic security audits and restrictions, the better to detect our adversaries. How well do such defenses work? At best, results are mixed. At worst, doing more of the same delivers results more promissory than substantive, while potentially alienating the average employee.

This report looks at the insider threat from a multi-disciplinary perspective. It reviews the literature on this subject and draws on Delphi research tapping seasoned professionals with broad career experiences. Ultimately, the report arrives at an alternative to prevailing wisdom. That alternative proposes taking institutional defense out of the realm of specialists and distributing the role more widely at the work team level. The proposed approach deputizes co-workers to take a hand in their own protection, as a co-pilot must be ready to fly a plane if the pilot falters. The resulting team-level engagement leaves fewer places for hostile insiders to elude scrutiny; hence fewer opportunities to prepare and carry out an insider attack.

"Given sufficient access and maneuvering room, trust betrayers can be devastating."

The Problem

The insider threat is an Achilles heel for critical infrastructure protection and the protection of any enterprise or institution targeted for destruction by adversaries. While risk and vulnerability assessments skyrocketed in the aftermath of 9/11, as reflected in the federal subsidies promoting them, the security focus centered largely on the vulnerability of large populations to attack (Masse, O'Neil, & Rollins, 2007, pp. 5–7). In this context, adversaries were characterized as traditional attackers working as outsiders who generally approach their targets head on with brute force–precisely in the manner of the 9/11 hijackers.

The insider threat, in this context, has been generally relegated to secondary status. One possible reason is that there is a dearth of statistically significant data on hostile insiders. As a review of the current literature indicates, trust betrayal—whether in espionage or other fields—remains statistically rare (Shaw & Fischer, 2005, p. 34; Parker & Wiskoff, 1991, p. 4).[1] When analyzed further, the insider threat has been subordinated to cyber security studies centering on hackers and disgruntled employees, ex-employees, or consultants (Brackney & Anderson, 2004; Cappelli, Moore, Trzeciak, & Shimeall, 2009; Leach, 2009). While such studies have supplied value and drawn attention to the problem, they have offered few solutions other than to advise continuing scrutiny. Data compiled to date suggest that the vast majority of insider cyber attacks have been either fraud-driven or moderate in scope and impact. In other words, such attacks remain less than devastating to the targeted employer–the modern, electronic equivalent of embezzlement or vandalism (Kowalski, Cappelli, & Moore, 2008, pp. 24–26). Similarly, such studies preserve their narrow focus by excluding cases of espionage, while at the same time avowing that the threat remains real and advising ordinary, more-of-the-same solutions like layered defense (Capelli, Moore, Trzeciak, & Shimeall, pp. 6–8). Consequently, it is difficult for security practitioners to derive new insights from cyber-centric insider threat investigations. The net result is that today's insider threat remains substantially as it did yesterday: often studied retroactively, yet seldom yielding practical tools, tactics, or recommendations that would serve a defender in countering the threat.

The overall aim of this study is to identify countermeasures that defenders can use to prevent terrorist attacks via trust betrayers and thereby reduce the vulnerability of critical infrastructure and institutions. The journey to this destination involves applying lessons of experts from other, more mature arenas of defense from insider threats, such as workplace violence, line management, corporate security, and counter-espionage. In the course of following this path, the study also explores one answer to the question, "If current indicators and countermeasures fall short, what should we do differently?"

1 Shaw and Fischer, looking at espionage as a subset of trust betrayal, argued that such trust betrayal appeared relatively rare, while betrayals by cyber insiders might be poised to be more frequent, hence more amenable to profiling and categorizing by subtype.

Terms of Reference

Throughout this report, the operational definition of **insider threat** is an individual and, more broadly, the danger posed by an individual who possesses legitimate access and occupies a position of trust in or with the infrastructure or institution being targeted. **Hostile** or **malicious insider** and **trust betrayer** also refer to the individual who represents an insider threat, although these two terms focus more attention on the individual than on the phenomenon. **Infiltrator** refers to a subset of hostile insider who sees himself or herself as an adversary prior to attaining insider status within the targeted infrastructure or institution. The infiltrator joins a targeted employer or group under false pretenses as a means of obtaining sufficient access to facilitate an attack. **Institutions** as used here refer to public and private sector enterprises, employers, entities, and organizations.

This report's focus is on the kind of hostile insider that poses an existential threat to the institution. Accordingly, this report is less concerned with overly broad definitions of insider threat that include malingering or contentious employees or naysayers who may pose a nuisance or cause difficulties for the organization yet stop short of bringing it to its knees.

Historical Approaches

The body of literature on the insider threat owes its existence to analysts of different areas of focus, as examined and sampled below. Psychological and sociological analyses of those who betray delve into motivations and enabling social contexts. Studies and historical documents related to espionage lean heavily on memoirs, historical compilations, and showcasing of flaws and pitfalls. More recently, emerging concerns over cyber security and susceptibility of critical networks to denial of service attacks have come to the fore in government-sponsored studies on insider threats.

Increasingly, government works appear to subordinate the insider threat to cyber security studies (Brackney & Anderson, p.32), centering on hackers and disgruntled employees, ex-employees, or consultants who cause damage via computer networks. While such studies have offered value and drawn attention to the insider threat, some have also limited their focus by concentrating exclusively on the specialized area of information technology (Kowalski, Cappelli, & Moore, 2008; DoD, 2000). Indeed, in their 2008 report to the President, infrastructure experts underscored this danger of focusing too intently on IT:

> Essentially, the threat lies in the potential that a trusted employee may betray their obligations and allegiances to their employer and conduct sabotage or espionage against them. Insider betrayals cover a broad range of actions, from secretive acts of theft or

> subtle forms of sabotage to more aggressive and overt forms of vengeance, sabotage, and even workplace violence. The threat posed by insiders is one most owner-operators neither understand nor appreciate, and it is a term that is commonly used to refer to IT network use violations. This often leads to further confusion about the nature and seriousness of the threat (Noonan & Archuleta, 2008, p.32).

Efforts to develop predictive models to detect and thwart malicious insiders have ranged from a quantitatively based yet unproven formula (Puleo, 2006) to broad-based theoretical models designed mainly to predict the triggers that lead an assassin or radical group to take violent action (Fein & Vossekuil, 1998; Olson, 2005). Others focus exclusively on detecting anomalous behavior in hindsight, on the assumption that trust betrayers are disgruntled and detectable by mistakes rooted in character flaws–while standing mute about infiltrators disciplined enough to avoid such mistakes (Leach, p.8). The literature contains much analysis on the psyches (Kaupla, 2008; Shaw & Fischer, 2005), social climates (Ben-Yehuda, 2001), and cyber vulnerabilities (Noonan & Archuleta; Kowalski, Cappelli & Moore) associated with malicious insiders. Yet analysis appears more limited on pragmatic lessons and inferential guidance that apply directly to practical countermeasures. However, research on threats from assassins to saboteurs suggests that applicable findings may be adaptable from indirectly related works and may offer more promise in charting a course to defending against the malicious insider who is more dangerous than a computer hacker (Fein & Vossekuil; Olson; U.S. Congress OTA, 1990).

"The threat posed by insiders is one most owner-operators neither understand nor appreciate, and it is a term that is commonly used to refer to IT network use violations. This often leads to further confusion about the nature and seriousness of the threat."

Types of Studies on Hostile Insiders

The literature elucidating the insider threat divides into three general categories: individual-centered studies focusing largely on psychological motivations or social context, case study compilations and cases that are mainly descriptive, and government-sponsored studies focusing largely on cyber threats. Table 1 arrays these various approaches in relation to one another.

Motivations

Those efforts that center around individual motivations and the psychological or sociological context of individual cases of insiders tend to dwell on underlying causes such as ideology, avarice, and social isolation.[2] While expanding their focus to look at the more modern phenomenon of insider threats that apply to cyber attacks, others who view the insider through a behaviorist's lens accord primary emphasis to stressors in the insider's life.[3] Even Ben-Yehuda,

2 For example, Bulloch, p. 151, dwells on the psychology of personal motivation to the point of characterizing traitors as sad individuals. Boveri, on the other hand (p. 13), in focusing on social context, takes the view that treason is a necessary precursor to radical change in all organized societies.

3 Shaw and Fischer epitomize this approach in their analysis of insider cyber threats, with the result that they accord primacy to personal stress as a dispositive factor, on pp. 15–20, possibly reflecting Shaw's bias as a clinical psychologist.

	Individual Motivations and Psycho-Social Context	**Descriptive Compilations, Cases**	**Government or Cyber Focus**
Focus	Insider as deviant Enabling social contexts	Sensational headlines Fatal flaws of defenders	Technology-driven controls Regulatory oversight
Counter-measures	Counseling, early intervention and rehabilitation, workplace hygiene factors	Inferential, i.e., reverse-engineered from finger-pointing at unseen vulnerabilities Awareness programs	Barriers to access, with emphasis on automation Process monitoring Compliance audits and quantitative models
Unaddressed Issues or Gaps	Accounting for why most others matching same profile do not become insider threats	Analytical examination of trends and patterns to contribute to prediction or mitigation	Pragmatic and pervasive solutions vs. narrow recommendations that focus mainly on imposing rules and monitoring compliance

Table 1. Insider Threat Categories of Research and Comparative Attributes

who has looked at individual cases in this framework and made historical compilations of numerous other cases of insider threats, notes that analysis of motivation and context alone provides unsatisfying answers (Ben-Yehuda, p. 110). Similarly, other analysts commented on the extent to which the "trust literature is dominated by" sociological approaches, which take issue with the limited value of studies that attempt to illuminate trust betrayal purely through focus at the individual level (Parker & Wiskoff, p. iii). Such studies fail to explain why the vast majority of people with similar pedigrees and circumstances neither betray their trust nor violate loyalties to become malicious insiders.

One sociologist looks beyond traitors and saboteurs to consider prisoner informants, Nazi collaborators, and whistleblowers as insiders whose status as betrayers ultimately rests on whether there exists a support group to back their actions, since "one cannot gain a hero or martyr image by oneself (Akerstrom, 1990, p. 50)."

Compilations and Cases

Studies with more of a multi-disciplinary approach show promise in shedding more light in this area.[4] Eoyang (1994, pp. 69–91), for example, notes that actions involving an insider's betrayal of trust are generally the result of calculation, not impulse. This dovetails readily with the observations of Allen and Polmar (1988, pp. 3 and 47), whose study of over 70 cases of insider betrayal left them characterizing the betrayers of the 1980s as motivated by "marketplace espionage" and otherwise appearing "faceless, unglamorous people" who were "seemingly ordinary." Others look at multiple cases over time, such as American traitors examined for more than 20 years by the Defense Personnel Security Research Center (Herbig, 2008, p. v).

Descriptive compilations and biographical narratives shift the focus to dramatic, anecdotal elements of cases of insider betrayal. Media accounts number among these kinds of stories, like a case involving an airport elevator mechanic who was allegedly abusing his access for 20 years to smuggle illegal aliens into Los Angeles (Weikel, 2008). Similarly, more sensational accounts of betrayal and capture, once ripped from newspaper headlines, lend themselves particularly well to timely compilation (as by Allen and Polmar), whereas analysis and application to

4 See Sarbin, Carney, & Eoyang who, like Ben-Yehuda, also focus attention on betrayal of trust and associated indicators that are relevant to arriving at a deeper understanding of malicious insiders.

countermeasures may lag.[5] A recurring theme in compilations is the showcasing of errors and failures in detection of foul play. The level and accuracy of detail varies in such works, and their didactic value is principally in highlighting examples of breaches to defend against and security gaffes to avoid. Thus, a KGB memoir looking at notorious American traitors such as the FBI's Robert Hanssen and CIA's Aldrich Ames reflects this insight:

> Intelligence officers might think they're chiefly responsible for recruiting agents, but most of the work really consists of finding people who want to be recruited (Cherkashin, 2005, p. 27).

Such memoirs occasionally reveal insights that only come after a long career in intelligence or counterintelligence, hence Wright's (1987, p. 301) conclusion that there is only one way to uncover the malicious insider. "Put him through an extremely thorough vet," probing through the insider's entire life and career, "until his secret life begins to unravel."

Even a short career as a case officer can yield complementary insights. A variation in the harvesting of lessons learned through memoirs comes from examining lessons designed for those whose job it is to seek out and exploit insiders. By inferring or reverse engineering guidance out of pitfalls, one case officer supplies this useful indicator: "Cover stories are what typically get agents into trouble (Waters, 2006, p. 81)." He goes on to explain how cover stories must be credible yet uncomplicated. This links the foregoing perspective of Wright, a senior British MI5 executive at the end of his career, with Waters, a fledgling CIA case officer reaching the same epiphany from a different vantage.

Sobering advice from practitioners takes many forms. It may not necessarily be encouraging for those interested in countering or intercepting insiders, as another memoir reveals:

> The KGB usually only found out about moles within its ranks when a Western defector, such as Edward Lee Howard, fled to our side with information about Soviet traitors (Kalugin, 1994).[6]

5 In the case of Allen and Polmar's book, for example, the cases mentioned answered the demand of a market created by *Time* magazine's label of 1985 as the "Year of the Spy," which fueled other commercial successes in this genre. One of these was Washington Post reporter Pete Earley's Family of Spies, which told the story of John Walker's compromise of classified codes to the Soviets while Walker served in the U.S Navy and of Walker's subsequent recruitment of family and friends to continue providing a stream of classified material for Walker to sell long after he retired from military service.

6 Kalugin, p. 202. Kalugin was an impromptu stand-in for a scheduled FBI speaker at a 2000 security conference in Washington, D.C. The FBI speaker was stuck in traffic while the former KGB general extemporized in fluent English on issues of the day. His wit and polish gave Kalugin the air of a Soviet version of William F. Buckley.

A unique variation of this theme is in Fishman's look at insider self-dealing and betrayal of nonprofit organizations, which leans heavily on compiling historical scandals. However, Fishman sees the promise of technology to enhance oversight by using web postings of audit trail data where the information becomes transparent and subject to scrutiny and action by "citizen-soldiers (Fishman, 2007, p. 310–311)."

Cyber Insiders and More Controls

Cyber security specialists, whose focus dominates current government studies on insider threats, observe that most insider cyber attacks have been either fraud-driven or reversible in scope and impact, i.e., less than devastating to the target (Kowalski, Cappelli, & Moore, 2008; DoD, 2000). It is thus difficult to rely on lessons focusing exclusively on cyber-centric insider threat investigations, if the objective is to defeat the kind of insider whose unimpeded attack could be fatal to the infrastructure or enterprise targeted. However, there are signs of a growing appreciation of the significance of the hostile insider as a potentially catastrophic vulnerability and some efforts to compare cyber and espionage cases, while acknowledging that most cyber attacks by insiders appear to occur after termination of employment (Band, et al, 2006, pp. 40, 52).

What remains unstated but may contribute to the self-limiting nature of cyber-dominated insider threat research is the influence of COBIT[7] standards on how information technology professionals handle security and compliance-related tasks. Consequently, recommendations for addressing the insider threat arising from this camp invariably speak of "controls," emphasizing the use of automated monitoring tools and technology to track and restrict network access. They also lean in the direction of generating more rules as conditions of use–the equivalent of lengthening software license agreements, which any computer user must acknowledge and accept prior to launching a given software application. The difficulty with these trademarks of the cyber security bias is not that they are valueless. It is that they may be insufficient or counterproductive. Adding the controls does produce an audit trail. This audit trail demonstrates due diligence. The proper display of due diligence then helps defend against charges of negligence after a breach occurs, thereby fending off faultfinding and finger-pointing campaigns. But just because a suite of controls prevents casual intrusion or hacker attacks by outsiders does not mean the same controls will stop a knowledgeable insider threat.

7 COBIT is an IT governance framework for addressing the combined requirements of controls, technology, and business risk. The IT Governance Institute first published COBIT in April 1996. Today COBIT emphasizes regulatory compliance in relation to IT governance. COBIT has become the standard for IT audits, particularly in rating compliance to the Sarbanes-Oxley Act of 2002. For more information on COBIT, refer to *http://www.isaca.org/Content/NavigationMenu/Members_and_Leaders/COBIT6/Obtain_COBIT/CobiT4.1_Brochure.pdf*

Losing Sight of Existential Threats by Aggregating Cases Too Liberally

Limits of Cyber-Centric Bias

Another pitfall in overemphasizing the cyber component in the growing body of government-sponsored studies on hostile insiders is analogous to the problem that workplace violence research suffers when its purview is extended to armed robbery. At present, the National Institute for Occupational Safety and Health includes armed robberies in compilation and reporting of workplace violence statistics.[8] Thus, while practitioners in this field may be interested in understanding and preventing rampage killings of the kind associated with either disgruntled employees or spillover of domestic violence into the place of business, their efforts are diluted by skewed data. The person who comes to the office and kills a boss and several co-workers is quite different from the criminal who shoots a convenience store clerk or taxi driver while conducting a hold-up at gunpoint. Yet the distinctions are lost when the cases are aggregated too liberally. This kind of aggregation can distort the picture of the insider threat when cyber attacks by hackers and mischievous teenagers are combined with seriously destructive sabotage meticulously planned and executed by a hostile insider whose aims and capacity for destruction are much more focused and lethal.

Finally, the cyber-centric lens can distort as much as it magnifies. One international observer studying in the context of defenses dating to the President's Commission on Critical Infrastructure Protection in 1996 and extending to post-9/11, uncovered a case of hyper reality as an outgrowth of over concentration on the cyber threat (Cavelty, 2008, p. 53). Specifically, Cavelty noted that a senior critical infrastructure protection adviser expressed shock that the 9/11 carnage did not originate from cyberspace, as that was widely believed to be the most likely source of the next attack (ibid). To this day, predictions of imminent catastrophic cyber attack continue to attract media attention as the next worst threat to come (Stein, 2010), yet they are often based less on statistically valid analysis than on surveys of cyber security practitioners at best providing "a rough measure of executive opinion (Baker, Waterman, & Ivanov, 2010, p. 1)."

8 This is why handling cash, dealing with the public, and delivering people or goods rate as high risk factors according to NIOSH. See *http://www.cdc.gov/niosh/violrisk.html* for more details.

Implications

Insider threat studies concentrating exclusively on hackers and cyber network attacks may risk skewing analysis and recommendations in the direction of adverse events that seldom represent existential threats to the organization. Even though such cyber adversaries may attain the equivalent of insider access and privileges once they have breached firewalls and cyber access controls, they are seldom true insiders. By Ben-Yehuda's construct (pp. 307–308), there is no treason if there is no corresponding betrayal of trust and violation of loyalty. So hackers and typical cyber attackers possess neither the trust nor loyalty that would qualify them as insiders. Nor do they possess the corresponding level of esoteric insider knowledge that would multiply the destructive power of their typical attack. Consequently, remotely based cyber attackers who are not insiders carry out actions akin to intrusion by stealth or outsider sabotage. What they may have in common with insiders is deception. But they are not fatal insider threats. Miscategorizing them distorts efforts to arrive at a common analytical core linking genuine insider threats to attack preconditions, their telltale signatures, targeting process, and susceptibility to detection and deception.

Similarly, over concentration on the sensational aspects of insider threat cases or on the psychological motivations and societal contexts of the act of betrayal are equally self-limiting. Their emphasis on the root causes of betrayal or on the idiosyncratic experience of a given malefactor soon become the primary focus, leaving security practitioners to fend for themselves in trying to infer useful security countermeasures.

The professional literature that covers this theme indicates that the insider threat is dangerous and often examined, only to be followed by calls for more study. The steady appearance of more studies and convening of groups such as Noonan & Archuleta's for a 2008 report to the President supports the argument that the insider threat to critical infrastructure continues to present a problem of national concern. What is needed is a level of insight that amplifies experience, which Leonard and Swap (2004) have defined as "deep smarts," the lens through which we now turn to a Delphi research effort for an alternative view.

Delphi Research on Insider Threat

The author's hostile insider studies began in mid 2008 as a social sciences research effort carried out under the rigors and oversight of the Naval Postgraduate School, Monterey, California. The research itself took place between January and April 2009, culminating in the author's published thesis on this subject. The research inquiry asked seasoned defenders, investigators, and line managers to answer questions and distill judgments through the iterative Delphi research process.[9] This project consisted of recruiting a dozen experts from different organizations and disciplines and asking them three series of questions over time. Respondents operated independently, with guarantees of confidentiality, and without any knowledge of or interaction with each other. After the first round of questions, respondents saw a compilation of all their answers and then addressed a second round of questions that were suggested by the first. Similarly, for the third and final round, respondents received compilations of their aggregate responses to the second round of questions in addition to a final series of questions informed by preceding rounds. This approach also followed the counsel of analysts who advised, "We need multidisciplinary research teams (not just geeks) investigating what we should look for as indicators of possibly malevolent behavior (Brackney & Anderson, p. 14)."

The group of experts in this study consisted of professionals representing different disciplines, with many having overlapping experience in fields such as

- Counter espionage
- Systems integration
- Operations management
- Fraud and threat investigations
- Critical infrastructure protection
- Prevention of workplace violence
- Local law enforcement investigations
- Human resources intelligence collection
- Workplace violence defense and response
- Defense against systemic institutional fraud
- Corporate response to handling reputational risk
- Federal law enforcement under cover assignments
- Crisis management and crisis information handling
- Management of public agency ombudsman functions
- Military service in combat and non-combat environments

9 For details on Delphi methods and utility, the reader may find an authoritative reference in G. J. Skulmoski, F. T. Harman, and J. Krahn, "The Delphi Method for Graduate Research," Journal of Information Technology Education 6 (2007), available at *http://jite.org/documents/Vol6/JITEv6p001-021Skulmoski212.pdf*. Readers unfamiliar with Delphi research and its application to this problem may question the legitimacy of the Delphi method, or even of all such qualitative methods in terms of their scientific validity. Appendix C attempts to answer these questions.

- Behavioral analysis and post-traumatic-stress interventions

Each respondent was selected, in part, for availability and, in part, for possessing

- At least 20 years of professional experience
- First-hand exposure to managing or investigating insider threats
- Current and foundational professional experience outside of each other's organization and unconnected to the researcher's purview, employment, or sphere of influence.

Each round involved transmitting and receiving questions by e-mail with at least two weeks between rounds. All respondents agreed to participate in the study under standard confidentiality protections and each signed an informed consent document, as part of an internal review board's oversight, consistent with contemporary social sciences research efforts. All the experts who agreed to participate in the three rounds of surveys saw the process through from start to finish, from January to April 2009 (Catrantzos, 209, pp. 6–10).

Initial Research Findings Confirming Accepted Wisdom

At the outset, Delphi experts suggested that traditional countermeasures, such as random audits, would offer high value in defending against a devastating attack. The experts independently converged on the accepted wisdom reflected in the foregoing literature review and represented in Table 2.

The worst insider threat initially seemed likely to be a disgruntled employee with (a) the capacity to plan a devastating attack and (b) the arcane knowledge to make the most of the opportunity (Catrantzos, pp. 5–38), upon further study this conclusion did not survive scrutiny. Indicators of the disgruntled trust betrayer included unexplained anger and other suspicious behaviors, like undue secrecy and self-aggrandizement, potentially serving as red flags. Similarly, countermeasures such as random audits, monitoring of employees, and vetting investigations appeared likely to offer value as

Table 2: Insider Countermeasures and Indicators First Suggested by Delphi Respondents

OBSERVABLE INDICATORS	COUNTERMEASURES
Undue secrecy Decline in performance Arrogance, displays of ego Own disclosures or revelations "Beat the system" talk, behavior Unexplained anger, behavior changes	Random audits Frequent duty rotations Background investigations and vetting Investigating reports of suspicious acts Technological monitoring of employees

Note: These indicators and countermeasures have no special order or correlation to each other.

Why Infiltrator vs. Disgruntled Careerist?

ways to thwart this kind of insider. By the end of the Delphi process, however, the same experts identified flaws in their own initial thinking. Their judgments countered the accepted wisdom and their own initial impressions of what constituted effective countermeasures.

Alternative Analysis Takes Shape

Three shifts in perspective and conclusions moved them away from the accepted wisdom. The first change came as a result of research questions that required the respondents to think like an attacker rather than a defender. This change made the respondents realize they could penetrate institutional defenses with relative ease. Second, out of this realization, experts determined that they could more usefully recruit, train, and direct an infiltrator rather than a disgruntled career employee. Finally, respondents arrived at recommended countermeasures involving a change of perspective: reliance on work team members rather than exclusive reliance on corporate sentinels, i.e., the institution's security, audit, and other specialists charged with watching for telltale signs of foul play.

For the respondents, one seminal, game-changing realization was that an infiltrator poses the greater threat if the goal is to inflict damage fatal to the institution. What supported this conclusion was agreement among respondents that existing defenses do little to foil the prepared infiltrator.

These expert observations dovetailed with some findings in the published literature. Specifically, traditional insider defenses appeared to be readily advised and just as readily circumvented. In fact, analysts making career studies of traitors, now extending their reach to cyber insider threats, continue to recommend measures that have yet to eliminate treason. Their recommendations include more awareness training for the work force, encouragement to report "concerning" behavior of fellow employees, and assigning individual risk values to these employees (Shaw, Fischer, & Rose, 2009, pp. 30 and 40). Some observers, basing their analysis on surveys of fellow specialists, also add automated monitoring by multiplying sniffer programs and computerized audit trails to more closely follow possible false steps of potential insiders (Garcia, 2009, pp. 2, 13). With a mindset recalling cyber aficionado shock at the low-tech nature of the 9/11 attacks (Cavelty, op cit), such observers see employees constituting the weakest link, thereby missing their potential as the first and possibly only line of defense (Garcia, p. 22). By intensifying countermeasures that have already proven ineffective, these observers may alienate not only

employees of the institution but their security staff as well. One cyber security analyst, however, swam against this tide. Examining the assumptions and computing the adverse results of imposing too many security controls, Microsoft researcher Herley raised eyebrows at a new security paradigms workshop in Oxford by suggesting that users often have sound, rational reason to reject security advice (Herley, 2009, pp. 1–12).

Epiphanies surfaced when the Delphi respondents independently admitted that the very countermeasures they had earlier recommended would present little impediment if they were the ones plotting the insider attack. The resulting consensus was that

- Infiltrators are the better choice for a terrorist seeking an insider for a devastating attack.
- Standard defenses in all but specialized environments (such as nuclear security) pose few insurmountable obstacles to an infiltrator.
- Under-exploited resources available within the average organization can be optimized to provide better protection against insider threats than sole reliance on security and other corporate sentinels.

Research findings suggested that the terrorist attacking as an insider would be more likely to be an infiltrator than a disgruntled careerist already in place (Catrantzos, pp. 11–41). A career employee with long-term access and detailed knowledge of inner workings may know more about how to dismantle critical assets than an infiltrator new to the organization. The same careerist, given time and planning, is in the best position to develop and carry out a devastating attack that circumvents defenses. However, the disgruntled insider is potentially unstable and difficult to control. According to the Delphi experts, this employee is not a joiner and is likely to be too self-absorbed to accept direction. Volatility makes this person an operational risk likely to compromise an attack out of disagreement with the particulars or out of spite at not being consulted on every move (Catrantzos, p. 26).

Additionally, target information for attackers remains highly accessible in the Internet age, particularly if the institution historically operated openly without the defenses available outside the national security arena. An institution's critical assets may also be immobile. Thus, in contrast to weapons classified for reasons of national security, critical infrastructure and institutions cannot be relocated or concealed once locations and operating details have been compromised. In this context, the targeting information necessary for mounting an attack need not be so esoteric as to be available exclusively to a career insider with very detailed knowledge.

Instead, as the Delphi experts reasoned, an infiltrator who gets through the door, even at a relatively low level for a limited time, should be able to accumulate enough details

Infiltrator's Challenges vs. Defender's Capacity

to enable an attack without having to spend years masquerading as an innocuous employee. Several Delphi respondents noted that many infrastructures and institutions have aging work forces and are desperate for talent. Another Delphi expert noted that average employers are prone to welcome skilled workers without criminal convictions who show an interest in accepting entry-level positions. The same employers make frequent use of contractors, who soon gain access to their systems. This situation gives an infiltrator two paths of entry: as a direct employee or as a contractor. Infiltrators may even try the two approaches concurrently without fear of one rejection contributing to another. In this context, if the remaining defenses are also flawed, the chances for a successful attack begin to tilt more in favor of an infiltrator than a disgruntled insider. The infiltrator may not have quite so much access, but can definitely be better controlled, focused, and more disciplined about concealing telltale indicators of an impending attack.

The weaknesses of traditional defenses against this insider threat appear more evident if depicted in the context of the mutual challenges of infiltrator and defender, as Figure 1 illustrates (Catrantzos, pp. 43–50).

Figure 1 depicts the situation in which infiltrator and targeted employer find themselves when these countermeasures and their limitations impinge upon each other in the traditional scheme of penetration and defense. In this conceptualization, the adversary's job is to select a target, prepare an infiltrator, and gain entry into the target to the point of being able to probe and maneuver with unimpeded access. It falls to the infiltrator to pass the background check and then enter and pass a probationary period. The probation period itself affords sufficient freedom of maneuver to gather information unimpeded by close scrutiny or interference. The infiltrator eluding detection or interference is free to operate in the dark corners of insufficient oversight and supervision, as long as his behavior and work performance do not deviate so much from the norm as to invite attention.

Infiltrator Step 1: Get Through Screening

The standard screening, or pre-employment, background investigation presents a low hurdle to the prepared. As long as the infiltrator does not have a record of criminal convictions or obvious disqualifications (like inability to lift twenty-five pounds in a job whose essential functions require some manual labor) he or she has little to fear

from the third party consumer reporting agency performing the background check.

The more invasive background and update investigations required for national security employment are not available for most employers, including entities operating the nation's critical infrastructure. Nor is it feasible to demand the same level of scrutiny for a maintenance mechanic as for an intelligence analyst. Besides, the telltale component of such investigations–the probe for financial irresponsibility–is only useful in cases where trust betrayal is primarily driven by money, exemplified in the so-called "marketplace espionage" most frequently observed in counterintelligence cases of the 1980s (Allen & Polmar, pp. 3, 47). However, as Herbig (2008) discovered in her study of trust betrayal in such cases over time, the trend in the last ten years has changed: the most common driver for today's traitors is divided loyalties, i.e., ideological rather than monetary motivation. Consequently,

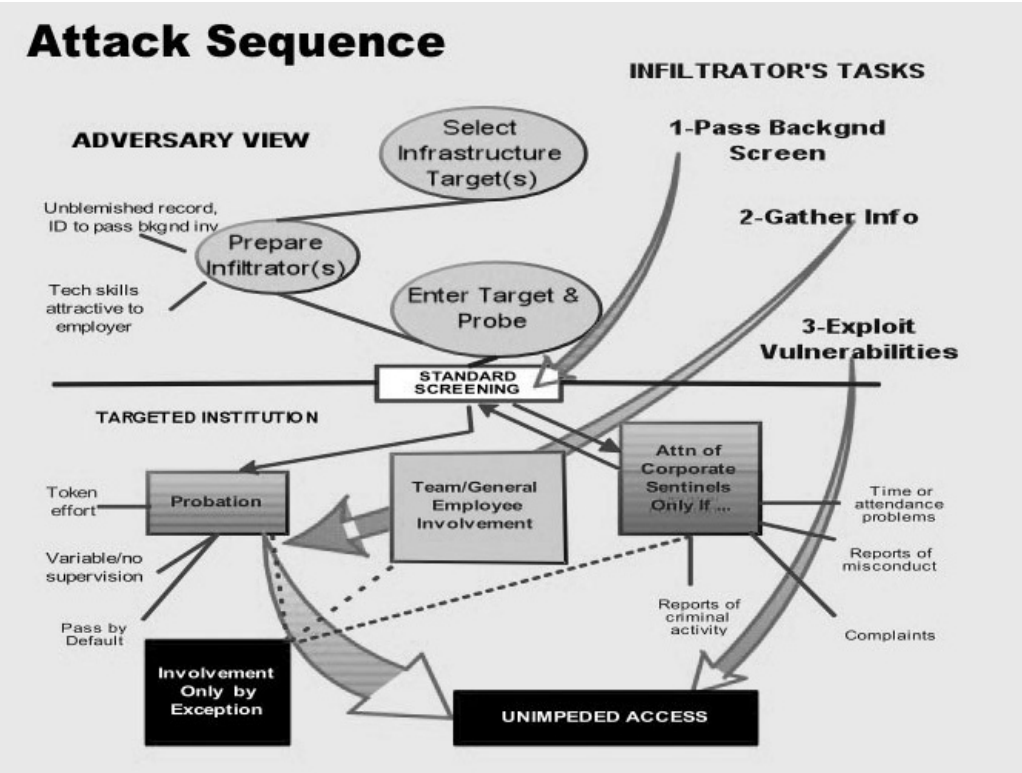


Figure 1. Traditional Situation: Infiltrator's Surmountable Obstacles

yesterday's focus on finances as an indicator of possible trust betrayal offers limited value in detecting today's traitors who may be living well within their means. Such trust betrayers may show no signs of the kind of debt indicative of financial hardship that could make them targets for bribery or ostensible candidates for selling out their employers to relieve financial distress.

Similarly, an infiltrator sent into an organization to attack it will be unlikely to draw attention by amassing bad debts that set off financial responsibility alarms, assuming a credit report is even requested or studied as part of the background investigation. Nor will this individual invite negative scrutiny through drunk driving or criminal convictions that the average background investigation detects through a standard check of superior court records in counties of residence and of employment.[10] Insulating the infiltrator even more from what such background investigations uncover is that the infiltrator is already under the control and sponsorship of a primary, albeit undisclosed, employer: the attacker. Thus, the infiltrator is seeking employment not so much for monetary or professional reward as for access to an assigned target. Meanwhile, the attacker coaches the infiltrator to avoid actions that would raise eyebrows. The larger and more sophisticated the attacker's organization, the more candidates are available to choose from in qualifying an infiltrator, and the more likely that the ultimate selectee will arrive on the job with an unblemished record.

To complicate matters more for defenders, the legal constraints affecting employers in the United States severely limit a critical infrastructure steward's ability to expand the scope of a background investigation or to use its product in any way that is not demonstrably related to a given job vacancy.[11] The same applies to any program for performing update investigations on existing employees. As one industry guideline cautions, "The consideration of extraneous information that is not a valid predictor of job performance can create a source of liability."[12] In the context of employment laws prohibiting job discrimination yet defending privacy, it is the rare hiring manager who dares flaunt such guidance by rejecting any otherwise qualified applicant, even if subtle or

10 In the United States, employment-related investigations can only legitimately use conviction records, not arrest records. Only law enforcement has access to the latter and is prohibited from sharing them with employers so that the latter do not unfairly affect an applicant's livelihood by making adverse hiring decisions before the legal system has decided actual guilt. See pp. 20–24, *Preemployment Background Screening Guideline* (Alexandria, Virginia: ASIS, 2006), http://bit.ly/preemployguideline.

11 Equal Employment Opportunity Commission, *Employment Tests and Selection Procedures* (2009), 1–6, http://www.eeoc.gov/policy/docs/factemployment_procedures.html.

12 *Preemployment Background Screening Guideline*, 24

stated antipathies against the United States surface during the hiring process. Fidelity to America is seldom called out as a hiring criterion for work at a utility that operates critical infrastructure or at any institution whose principal business does not involve national security. In the broader context of employment law, anti-discrimination protections, and limitations on the extent to which employers may practically scrutinize applicants for work, background investigations are unlikely to unmask any but the most unsophisticated of infiltrators.

Update investigations, if performed at all, typically come after seven years because this is the standard limit that many states and the Fair Credit Reporting Act recognize as the maximum period for making criminal history available for retrieval for employment purposes.[13] Like preemployment investigations, updates performed through a credit bureau or other agency falling under the rules of this Act must also be fully disclosed to the subject of the investigation. An infiltrator requiring more than seven years to gather insider information to support an infrastructure attack may have aged enough to cast doubt on his or her motivational zeal or be suspected of identifing too closely with the target.

Infiltrator Step 2: Gather Information

As Figure 1 shows, once safely through the door the infiltrator now interacts primarily with fellow employees and a supervisor, who supplies the institution's direct oversight during the probationary period. Corporate sentinels, whether security staff, auditors, information systems guardians of the computer network, human resources recruiters, attorneys, or others with assigned responsibility for various monitoring functions, may rarely interact with the new hire. The new employee benefits from a grace period during which minor transgressions committed in the course of gathering information are often dismissed as a rookie's excusable faux pas. Unless the new hire does something egregious to excite remark, he or she is unlikely to face a random audit, active monitoring of computer key strokes, or time and duration of access into a given work space. On the occasion when an infiltrator's actions invite challenge, all that may be necessary to deflect focused attention of corporate sentinels is a ready apology and a profession of ignorance.

To further limit opportunities for detecting an infiltrator's suspicious gathering of insider information via random audit, Delphi experts in business and operational audit noted that so-called random audits are seldom truly random. As one of the respondents pointed out, the astute observer sees them coming. Moreover, many audits are perfunctory, particularly if auditors are overextended and disinclined to take on the extra work of sustaining a negative finding. As one analyst found in a longitudinal study of organizations susceptible to accountability failures, cases are "resource intensive and, as a result, enforcement is necessarily selective (Fishman, p. 274)." This may explain why a

13 Ibid., 20 and 22.

resource-intensive audit will not be "wasted" on a new employee who has still not even passed probation.

In many, if not most organizations, audits are by definition adversarial. Regarded as a necessary evil, auditors may struggle to obtain active cooperation. One Delphi expert noted that co-workers are even more likely to defend than to report a trust betrayer who has managed to come across as "just one of the guys." The greater scrutiny is likely to focus on activities affecting financial performance or high-value losses. However, until the moment of attack, the infiltrator targeting critical infrastructure may be unassociated with any loss-producing events that would invite such scrutiny. In such circumstances, it is the rare audit that will identify and focus sufficient attention on an infiltrator to elicit anything more than an oral warning or mild rebuke. Consequently, the traditional audit poses little threat to the infiltrator operating with some degree of training and sophistication.

Technology exists to remotely monitor every keystroke an employee makes whether operating a desktop computer or a supervisory control and data acquisition (SCADA) system–the principal means of controlling valves and distribution of signals, power, or water when handling a critical infrastructure component. It is possible to configure control room access so that no one individual may enter a critical area alone. It is also possible to monitor such areas remotely through video surveillance. These capabilities can theoretically prevent all but the most astute from carrying out undetected acts of mischief. However, when applied to the challenge of detecting and thwarting an infiltrator bent on attacking critical infrastructure, technology alone falls short for several reasons.

For every device capable of tracking activity, there must exist somewhere in the institution a means of distinguishing suspicious activity from acceptable routine. A surveillance camera or automated log cannot by itself tell whether an operator laying hands on a SCADA panel is doing his job or interfering with another's. Such a determination requires human judgment. True, some automated tools can approximate a level of human judgment, if given precise details and parameters of what kind or number of transactions become suspect once they exceed a certain frequency in a given time period or take up significantly more time than necessary. However, the effort needed to establish these boundaries and the resources necessary to automate associated triggers may exceed the capacity of the average employer. Nor is this investment in proportion to the expected benefit.

The same caution applies to the labor-intensive alternative to this technology-based solution: invasive oversight by a designated monitoring force. Delphi respondents with career experience as line managers in critical infrastructures opined that such "snooping" negatively affects productivity and morale, while often leading to an unintended consequence. It sparks the creativity

of aggrieved operators to find new ways to elude or defeat monitoring systems because they dislike being watched like wayward children.

Undermining such corporate sentinels, whether human overseers or automated devices, soon becomes part game, part badge of honor. Co-workers transfer this knowledge of how to bypass what they regard as invasive monitoring to peers and newcomers alike–including the potential infiltrator–because they know that if all the workers are defeating Big Brother, then management will be unable to single out any one employee for punishment.

Infiltrator Step 3: Exploit Vulnerabilities

At this point in the penetration effort, if the infiltrator has managed to survive the screening process and stay under the radar of corporate sentinels, inertia and initiative are on his side. The more he blends, the less he stands out, and the more likely he is to gain the unwitting support of co-workers and management alike, particularly if seen to be a competent team player who gets along well with others.

One contradiction in defensive strategy highlights how traditional measures can be self-undermining. The common thread that unravels the foregoing defenses when exploited by an infiltrator or any hostile insider is a lack of active involvement on the part of the workforce on the one hand, tied with what infrastructure workers perceive as the offensiveness of too much oversight on the other hand. One career analyst of trust betrayers explained the latter phenomenon by stating that vigilance against disloyalty "threatens the ecology of trust and raises the likelihood of disloyalty because of a motivation to resist excessive oversight (Carney, 1994, p. 21)."

In this framework, the institution comes to rely excessively on its corporate sentinels, namely, its designated watchers, such as security staff. The rest of the workforce may be indifferent to the defensive role that employees and managers have ceded to specialists. Meanwhile, the capacity of the sentinels to focus limited resources on discovering a needle-in-the-haystack level of visibility of an insider threat is constrained by average employee resistance to draconian security measures that are costly and impede operations. Into the space between general employee indifference and constraints on corporate sentinels, the infiltrator and any insider threat can create a dark corner to carry out hostile activity with impunity, as Figure 1 illustrates.

The Alternative

One way to overcome Figure 1's vulnerabilities is to re-examine the infiltrator's penetration sequence in light of how a different strategy might apply the same institutional resources to better effect. Figure 2 shows such an alternative end-state.

What has changed? First, the screening process no longer relies on a search for indicators that uncover neither infiltrator nor other hostile insiders. As one executive who studied trust betrayal for their entire career pointed out, many experts find that personnel investigations do not prevent espionage or detect those who may commit such a crime (Anderson, 1994). Instead, the process now pays special attention to verifying identity. It takes advantage of government resources through a program that U.S. Immigrations and Customs Enforcement (ICE) makes available to companies and infrastructure institutions alike—ICE Mutual Agreement for Government and Employers (ICE/IMAGE). For a fraction of the resources necessary to conduct update investigations of utility employees every seven years,[14] employers can instead devote more attention to verifying basic identity and right-to-work authorizations of new hires in order to defend against potential infiltrators. They improve their internal capacity for such detection by availing themselves of a federally funded program that trains human resources recruiters to check credentials and gives them access to Social Security and immigration databases to facilitate verification of employment eligibility (*ICE Mutual Agreement for Government and Employers*, 2010).

The new screening program will not catch all infiltrators or defeat individuals who enter the institution benevolently and only later develop hostility and a propensity to betray or destroy. However, the program could reduce the ability of terrorist organizations to infiltrate their agents with falsified credentials. This is why Figure 2 shows a smaller X next to the arrow depicting the infiltrator's first task. The new screening program may complicate the challenge for the infiltrator, but does not eliminate it altogether.

More importantly, however, the biggest change from the Figure 1 traditional approach to the Figure 2 alternative is the active engagement of the general employee population. Employees participate in the screening process by verifying credentials through their own professional and trade networks. The immediate supervisor monitors the employee closely throughout the probationary period. During this interval, the new default expectation is not that all newcomers pass probation absent egregious incidents, but that all are released from probation unless they demonstrate talent worth keeping. This demonstration must satisfy not only the supervisor but teammates as well, which encourages close interaction on a daily basis.

14 The seven-year number is based on the standard state limit for reporting of criminal convictions and that the Fair Credit Reporting Act uses for employment-related background screening (*Preemployment Background Screening Guideline*, pp. 20, 22).

Moreover, during probation, new hires are treated like student pilots who are not ready for solo flight—never left alone in the cockpit. Only, in the case of critical infrastructure, the student is a new employee and the cockpit is any critical asset or control system. At the same time, this alternative approach requires a culture of constant team interaction and self-monitoring that reduces opportunities for probing and undermining the institution clandestinely. It reduces the dark corners represented by the black boxes in Figure 1 because, in Figure 2, employee oversight means there are fewer places to hide. This is the No Dark Corners approach that configures the job to reduce chances for a sole individual occupying a sensitive area undetected. It aligns with the security prescription of management expert Tom Peters who exhorts security professionals

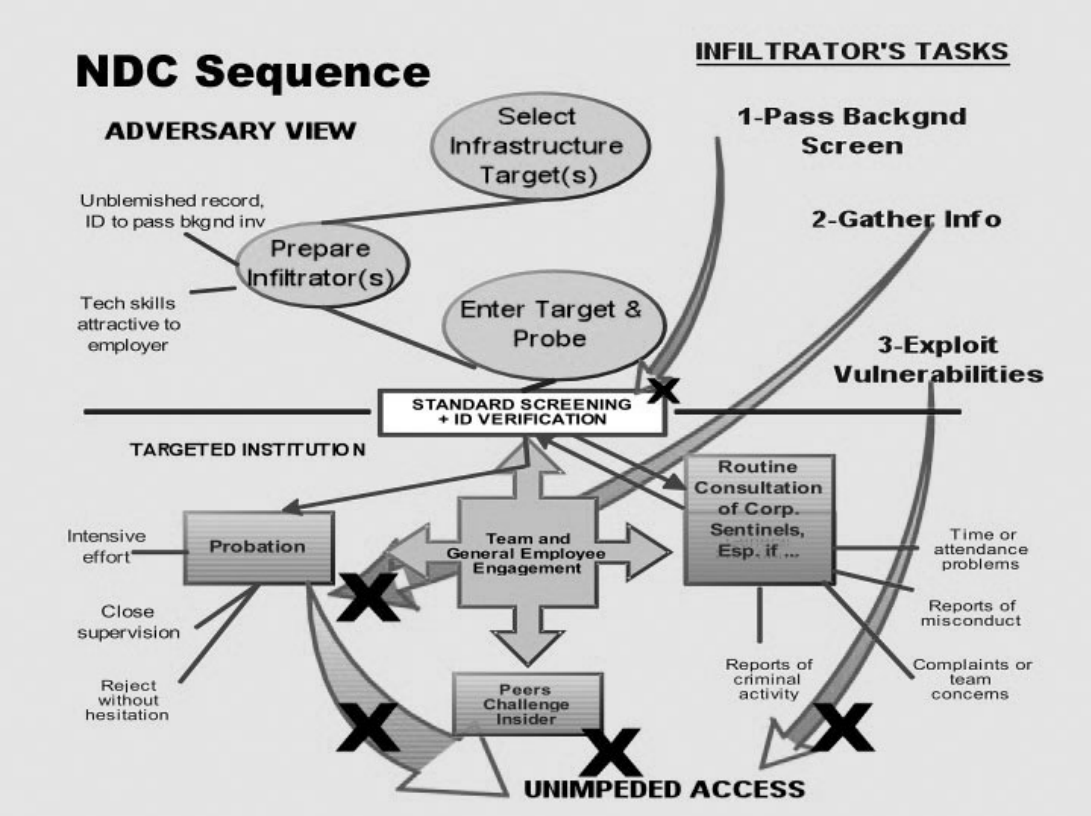


Figure 2. Desired End-State for Defense from Hostile Insider

Balancing Trust and Transparency: The Co-Pilot Model

not to see their contribution exclusively in the character of corporate sentinels:

I don't want you to be security people for the organization, but to make everyone else in the organization a security person. You don't "do" security. You help all the employees do it…You win the game when I and my colleagues are the real security people in the place (Peters, 2007).

This alternative approach may increase the opportunity to detect insider threats because it spreads defensive responsibility pervasively, rather than relying exclusively on corporate sentinels.

How can a cultural shift in the workplace create a team whose members constantly monitor each other without undermining the trust vital for group cohesion? On the surface, it would appear that such a team is merely relieving assigned corporate sentinels of their oversight duties. After all, as organizational consultant Stephen Covey has observed, suspicion can generate the behaviors that managers and leaders are defending against, thus fostering a collusive environment of distrust (Covey & Merrill, 2008, p. 292). Extending the co-pilot and cockpit metaphor from the preceding discussion on probation, however, offers an answer to this apparent contradiction.

In line with the shift to internal team monitoring, every team member becomes not an inquisitor but a co-pilot. Each member exemplifies the elements of the co-pilot definition of a "qualified pilot who assists or relieves the pilot but is not in command (Merriam-Webster, 2009)." The co-pilot maintains a vested interest in maintaining safe altitude and air speed and in arriving on schedule at the right destination. Applied to the work team, this model makes every team member a co-pilot. Both a team member and co-pilot should be in a position to fully monitor what is happening in the cockpit or control room, with aircraft gauges or with SCADA displays. In this context, a co-pilot level of engagement becomes cohesion producing because it demonstrates a shared sense of ownership in the team's work. As an added benefit, engaging employees in a

Contrast with Traditional Strategy

more collaborative endeavor such as this offers a way to relieve what some management analysts characterize as the "deadening impact of routine (Vermeulen, Puranam, & Gulati, 2010, p. 73)."

While many parts of a given countermeasure carry forward into the new framework, the means of applying the countermeasure changes fundamentally. This approach can transform techniques into performance gauges for work teams. A video camera monitoring a critical process involving hazardous materials could now be seen as a way for a fellow team member to summon assistance if another team member in the area gets hurt—not as a spy camera for supervisors to catch subordinates in the act of violating established procedures. The same cultural shift could make team members appreciate having a back-up control room operator or lineman within earshot or line of sight. Embracing the co-pilot model could transform additional physical or electronic monitoring into a means of summoning assistance. It also limits opportunities for a hostile insider to act against the institution. Ultimately, greater transparency and work redesign may limit opportunities for clandestine and damaging activities by eliminating the dark corners that insider threats need to do their worst.

Applying the new strategy communicates to the would-be insider threat that someone may be watching. In a traditional approach, the watcher is a corporate sentinel, and there are seldom enough watchers to monitor every process or venue. By contrast, in a No Dark Corners setting, the one who may be watching is a co-worker who has a proprietary interest in a job, a work team, and the institution, and will therefore act to defend them.

Key to this strategy is not only innovations but also what management expert Peter Drucker emphasized as a primary duty of all organizations: organized abandonment of processes and strategies that are no longer working (Drucker, 2002, p. 295).

Measures that impede an infiltrator's ability to surveil or strike take precedence over measures that are easily bypassed and may offer negligible value in defeating an insider threat. Organizing these measures to contrast them with the traditional defenses that accepted wisdom favors underscores even more the distinctions of the new approach. Figure 3 presents this contrast in the form of a strategy canvas where the traditional approach appears in red and a breakaway challenge to this strategy appears in blue.

The strategy canvas offers a gauge and a framework for revealing where traditional insider defenses have faltered and where innovations may offer alternatives to reduce chronic vulnerabilities.

New Insider Defenses

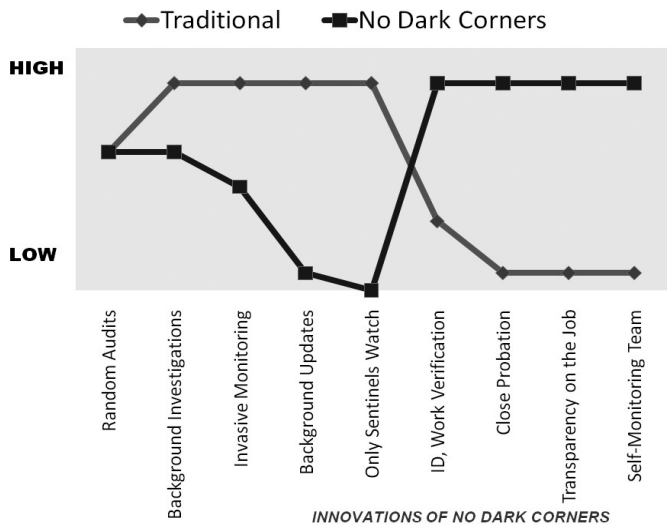


Figure 3. Strategy Canvas: Traditional vs. No Dark Corners

The canvas depicts the current state of affairs in insider threat defense (in red) as well as the potential (in blue) to reduce susceptibility to infiltrators and, by extension, to any hostile insider.

In addition to adjusting defensive measures already discussed, Figure 3 draws attention to three particular innovations that reflect insights both of Delphi respondents and of published analysts of trust betrayers. These three are close probation, transparency on the job, and team self-monitoring. All three measures offer productivity as well as defensive benefits.

CLOSE PROBATION. In a paper published in the *Harvard Business Review*, the authors state "organizations that systematically integrate new employees enjoy lower turnover, and the recruits report greater commitment and job satisfaction (Fernandez-Araoz, Groysberg, & Nohria, 2009, p. 84)." This, as well as other tools could defeat hostile insiders through the scrutiny of a co-worker, or what one analyst calls a "citizen-sentry (Fishman, p. 311)."

For some organizations, probationary periods are a means of rejecting a new hire before work rules confer the equivalent of tenure or life-time employment. However, some Delphi respondents reported that the probation process is seldom properly exploited. Hiring managers may hesitate to let probationary employees go, particularly if the hiring process was lengthy and demanding. The Delphi experts reported that the longer a vacancy goes unfilled, the greater the chance of losing that position, as upper management can see work getting done despite the vacancy. In addition, some respondents noted that where mentoring and monitoring of new hires are deficient, hiring managers tend to keep new hires

past probation by default, to give them the benefit of the doubt. The No Dark Corners approach puts a premium on using probation as originally designed. The default shifts away from keeping the new hire absent flagrant misdeeds. Instead, the new default becomes termination at the first sign of misgivings and automatic release at the end of probation absent outstanding performance. The only way to keep a probationary hire becomes via the support of front-line supervisors and fellow members of a work team. The supervisor acts as the pilot, with the rest of the team as co-pilots—all having a vested interest in assuring that anyone joining their ranks can be trusted in their institution's equivalent of the cockpit.

TRANSPARENCY ON THE JOB. In keeping with the new approach for maximizing the value of probationary periods, transparency on the job means that every task, operation, or action performed at a critical infrastructure site should be within the actual or virtual line-of-sight of a knowledgeable peer or supervisor. Evoking the two-person-integrity rules of working in some classified or nuclear environments (Honnellio & Rydell, 2007, p. 218), every job and work space should be designed to maximize visibility to peers and minimize opportunities for clandestine, hostile action.[15] While critical infrastructure employers seldom have the staffing to implement a forced buddy system like this under all circumstances, the selective use of surveillance cameras to monitor critical operations can at least reduce infiltrator assurance that clandestine activities will remain undetected. The deterrent value of this kind of system is analogous to that of having surveillance cameras and their associated video monitors openly placed near the cash register at retail convenience stores. This practice in retail security is thought to deter robbery because of the uncertainty it creates about who may be watching in the eyes of the potential robber (Nieto, Johnston-Dodds, & Simmons, 2002, p. 34; Murphy, p. 19, 1999).[16] Process-monitoring cameras, which assist with environmental watching of systems to be sure

15 This recommendation recalls an unrelated but complementary observation that the corporate security director of a retail fast-food corporation shared with the author. Specifically, the director noted that his greatest value to his employer came as a result of close integration with the business, because he required each of his staff members to spend time in one of the stores. Consequently, when security came to design the operating manual for opening and closing each retail establishment, the security director was able to integrate secure cash handling and loss prevention procedures into day-to-day operations instead of trying to add them as an appliqué. Losses from both internal theft and armed robbery declined as a result.

16 Patrick Murphy, Loss Prevention Director for Marriott International, confirmed experiencing an 84% decline in losses from armed robberies as a result of such an openly visible installation of surveillance cameras, which led him to publish his experience as an industry best practice in 1999 and which still held true ten years later (personal communication, July 23, 2009).

they are operating within design tolerances and of hazardous areas in order to dispatch rescue crews, are already commonplace at infrastructure sites, as are security surveillance cameras and access control systems in public areas, particularly in Britain.[17] Designing new work sites, as they come online, to increase such visibility reduces the perception of concealment opportunities and increases the opportunity for fully engaged team members and other employees to spot untoward activity while routinely looking out for each other.

17 See p. 16, Nieto, Johnston-Dodds, & Simmons, op cit, and R. Day, Remotely Monitored CCTV Reduces Theft by 80%, in Secure Times, Essex, UK: Sheen Publishing, Ltd., May, 2009, p. 19. Richard Day, a manager whose British firm had been experiencing high losses of construction equipment to burglars, credited remotely monitored surveillance cameras for reducing such losses by 80% as of June 2009.

TEAM SELF-MONITORING. Finally, the new alternative recognizes and seeks to exploit the difference between over-the-shoulder audits and self-policing out of work team cohesion and pride. As one Delphi respondent observed, the most effective use of audits occurs when internalized at the work team level. Instead of shrinking from oversight as a form of witch-hunt, team members focus on "how we can make things better" discussions. By including such discussions in regular team meetings and also encouraging informal one-on-one comments between employee and supervisor after each formal meeting, members should become their own most ardent diagnosticians. This self-monitoring presents an imposing threat of discovery for the infiltrator who may be adroit in hiding from corporate sentinels but cannot hide from the team.

"Instead of shrinking from oversight as a form of witch-hunt, team members focus on 'how we can make things better' discussions."

Comparison with Other Security Strategies

As another Delphi respondent noted, metrics by themselves may supply only an illusion that management can track all work and make necessary course corrections in time. As a senior executive in a large infrastructure organization, he did not have time to read let alone check for discrepancies in employee performance based on all the timekeeping, output measures, budget variance, and failure analysis records available only to senior executives. So, this expert pushed out these data to front-line managers who could at least track themselves and their own team. As a result, the managers and soon the team members started gauging themselves and monitoring their own performance, improving effectiveness in the process. Some teams competed with each other in friendly rivalry. More teams and their managers, though, began competing with themselves, striving to beat last month's or last year's best record. One Delphi expert reasoned that this kind of self-monitoring, properly encouraged and applied to defense against insider threats, could present an almost insurmountable obstacle to infiltrators intent on an attack against critical infrastructure. Within a general management context, independent management studies on trustworthiness also confirm this view that few approaches rival the effectiveness of anomaly detection by peers in a social network (Ho, 2009, p. 6) or even the value of management-employee communications in deterring sabotage in business settings (Giesberg, 2009, p. 2439).

The new strategy of configuring work space for maximizing opportunities for teammates to exercise a proprietary interest in their work and for promoting transparency relies on employees—legitimate insiders—defending an institution and its infrastructure by taking ownership. No Dark Corners is to critical infrastructure what Defensible Space is to community housing and Fixing Broken Windows is to community policing: a defensive strategy relying on legitimate users of a given space to exercise a proprietary interest sufficient to defeat adversary encroachment. In his seminal work, Defensible Space, architect Oscar Newman examined data from housing projects in New York to make a case for reconfiguring residential areas to enhance the natural human tendency of territoriality. In his words, "defensible space is a model for residential environments which inhibits crime by creating the physical expression of a social fabric that defends itself (Newman, 1972, p. 6)."

While Newman made efforts to extend his work to nonresidential environments with government sponsorship, the latter appeared to make little progress in the course of 20 years, despite considerable investment.[18]

18 O. Newman, personal communication, November 21, 2002. Newman's remarks came in an e-mail response to the researcher's inquiry regarding whether he was still teaching his principles or aware of any such program of instruction he would currently recommend for security practitioners.

In a variation of Defensible Space applied to order maintenance in public spaces, James Q. Wilson and George Kelling offered Broken Windows theory ten years later (Wilson & Kelling, 1982). Then Kelling's follow-up research demonstrated multiple successes in crime reduction in major urban cities—all based on the premise that neighborhoods decay into crime and disorder if the little things, like broken windows, remain untended (Kelling & Coles, 1996, p. vx). Conversely, attention to the little things, like fixing broken windows, sends a communal message of a sense of ownership. This demonstration of proprietary interest, in turn, deters offenders, driving them away from protected areas.[19]

No Dark Corners extends the foregoing theme of a sense of ownership to critical infrastructure, in a way that recalls the housing application of Defensible Space and the community order maintenance of Fixing Broken Windows. The difference is that while the other two models apply exclusively to public spaces, the new approach adds private space into the mix, as all critical infrastructures and most institutions have control rooms or physical assets that are not open to the public, hence, out of the public view. Invariably, however, some important assets remain exposed, such as transmission lines, reception areas, and aqueducts, which may be visible or accessible to members of the public.

Why has the new alternative not surfaced before? According to observers of organizational cultures under stress, whether induced by sabotage, terrorist attack, or workplace violence, "denial is a powerful feature of organizational culture; it prevents sense making when crises appear (Wang, Hutchins, & Garavan, 2009, p. 35)." Moreover, many if not most organizations and institutions operate within the private sector. By extension, their critical assets must therefore be under private rather than public control, hence beyond the reach of the earlier models that rely on stimulating a sense of ownership exclusively

19 Kelling's theory is not without its critics. However, much of the criticism is directed not at whether Fixing Broken Windows works to take back public spaces from offenders who otherwise scare away legitimate users of the public, but at larger societal issues, such as the inevitable displacement of offender activity that occurs in neighboring communities that are not using the same strategy. The criticism is along the lines that applying Broken Windows just pushes a problem from one neighborhood to another. Similarly, other critics object that changing demographics may also account for crime. Since Kelling did not offer his theory as a panacea or as the sole explanation for decreases in crime, himself taking account of other factors, including Newman's work, it is more accurate to say his theory may have been challenged but not discredited. More recent criticisms focus on community policing aspects of the theory, which vary greatly depending on the police force. However, as researchers Braga and Bond highlighted, this point vindicated the theory in a recent study, which found that cleaning up the physical environment in Lowell, MA, was very effective, while a corresponding increase in misdemeanor arrests was not (C. Y. Johnson, Breakthrough on "Broken Windows." Boston Globe, February 8, 2009. Retrieved July 5, 2009).

in public areas, like Defensible Space and Broken Windows. To complicate the protective challenge further, critical infrastructure and institutional assets may extend across both public and private spaces. Many of them are difficult to secure in the traditional sense. For example, transmission lines, aqueducts, and fiber-optic cables stretching across broad expanses of undefended territory hardly lend themselves to being kept under the control of locks and intrusion alarms. Moreover, in a world of increasing complexity, it may well be that modern society has come to over rely on specialists, for fear of burdening the general work force or risking errors. We perpetuate self-imposed limits by advising the average employee to leave it to the professionals. Thus, catching insiders, in this mindset, becomes the work of specialists who fill the ranks of corporate sentinels. However, as a recent British security guide has demonstrated, true stakeholders consist of anyone who has an interest in the operational security of the site, including security staff, occupants, and operators (Centre for the Protection of National Infrastructure, 2010, p. 4). Involving the entire community of stakeholders in its own defense can significantly extend the protective reach of corporate sentinels.

How does a security practitioner implement the new approach? Every manager and innovator must operate within the opportunities and constraints created by that individual's own management and organizational culture. Ideally, the practitioner operates in an environment receptive to innovation and to a business case which aligns the co-pilot approach of insider defense with improved productivity and team work. Recognizing that security practitioners seldom operate in ideal circumstances, one must look to take advantage of opportunities for pilot programs and even incremental change while identifying and cultivating an organizational champion. Management authority Peter Drucker advised introducing new approaches via a low-risk pilot program to allow the institution an opportunity to get acquainted with changes while giving innovators the chance to fine tune the program to handle unexpected complications. Nevertheless, there may be circumstances where an organization is unreceptive to a pilot program or where the security practitioner is unable to obtain enterprise-wide support for those aspects of the program that fall beyond his or her authority, such as modification of the employee probation process. In such conditions, an incremental approach may still offer opportunities. One may not be able to change the entire probation process, yet still modify how one's own department takes advantage of that process. If successful, one may then influence other departments with like-minded allies to pay closer attention to the probation process as a way of avoiding the potential consequences of poor hiring decisions. Similarly, by making the most of the security department's organizational discretion and by using the strategy canvas (Figure 3) as a guide, one may gradually shift managerial emphasis to give greater priority to key features of the new approach. Finally, as with implementing

any security program, it may be helpful to identify an advocate or champion from top management who can see the value in the alternative approach and offer counsel and support in instituting necessary change.

No Dark Corners shifts exclusive reliance of institutions from corporate sentinels to the larger employee population, especially the work team closest to the infiltrator or other hostile insider. It also redirects some investment away from moderately useful preemployment background investigations and update investigations, which may deter obvious criminals but might not defeat a hostile infiltrator.[20] Instead, the strategy shifts this investigative scrutiny to verifying identity and right-to-work documentation, which takes the form of supplemental identification, and which the Immigrations and Customs Enforcement arm of DHS is advancing through its ICE/IMAGE program of enhancing the capacity of all employers, including infrastructure stewards, to

20 Basic preemployment background investigations continue to offer value as a tool of due diligence that may detect or deter criminals and individuals with a history of misconduct. They do not pose a serious obstacle to a moderately prepared infiltrator whose selection may depend on a history free of criminal convictions and other easily identifiable discrepancies that background checks are designed to spot.

"...this new strategy brings to bear the tools of close probation, work redesign for transparency, and self-monitoring for greater engagement of the employee population and, in particular, the work team."

Conclusion

close the door to a major penetration vulnerability in the hiring process (op cit).

At the same time, this new approach brings to bear the tools of close probation, work redesign for transparency, and self-monitoring for greater engagement of the employee population and, in particular, the work team.

In a No Dark Corners workplace, standard screening will have new emphasis on identity and right-to-work verification. False credentials will be increasingly subject to discovery, making it difficult for a foreign adversary to penetrate an American institution. Close probation means an infiltrator will face constant scrutiny, supervision, and evaluation. Similarly, a fully engaged employee population and work flow design that eliminates hiding places while promoting transparency will reduce opportunities for the infiltrator gathering sensitive information and breaching protocols under the banners of ignorance or deficient supervision. Corporate sentinels will be accessible to team members to follow up on their concerns and suspicions. In the process, the sentinels themselves may become part of the extended family seen as supporting the work team. Opportunities for unfettered, clandestine access will be severely constrained, subject to monitoring by people or devices, and too limited to exploit reliably. Appendices A-C offer suggestions for introducing this approach into the workplace.

All a hostile insider needs to carry out an attack are access to a worthy target, an open door, and a dark corner from which to plot and maneuver. Any adversary seeking to strike a devastating blow against any institution need look no further.

Public and private sector institutions and critical infrastructures number among the many worthy targets, as would any organization with critical assets to be defended. The potential for loss does not always stop at the door of one target, however. Not only are some targets like infrastructure irreplaceable, their damage or destruction may lead to cascading failures of other, interdependent components, from banking and finance to emergency responders, from transportation and logistics to food and agriculture. All depend on electricity or water or communications–the double-edged sword of living in an interconnected world.

The open door comes from a traditional culture of openness and few restrictions to movement or assets in the average workplace. This openness flourishes because local government agencies and investor-owned organizations alike must answer to demanding stockholders, ratepayers, and various regulatory agencies. Even when these organizations have critical assets to protect, when it comes to their public customers, they cannot be perceived as having something to hide. In this environment, defenses against infiltrators or any type of insider threat require a cultural shift. The challenge is to close the door

to infiltrators while leaving it open to legitimate workers and business.

Even if an infiltrator sets sights on a worthy target and exploits weak defenses, he or she still needs a dark corner free of oversight in order to gather pre-strike intelligence and then initiate an attack without risk of timely intervention and defeat. The best way to defeat such an attack is to remove the dark corners.

Our society's reliance on technology and specialists to solve problems can marginalize the average employee, excluding him or her from playing a useful and necessary role in insider defense. Employees should be recognized as the first line of defense, bringing them onto the front lines with a No Dark Corners approach. Consequently, in addressing the insider threat, we must reconsider our usual efforts to penetrate with the intensity and focus of a laser what we should instead be illuminating with a flashlight. No matter how deep the laser drills, it points to only a fragment of the entire picture. Caught in the laser's beam, a clever insider can mask or explain away hostile activities with relative ease. The same malicious insider, however, cannot deceive alert peers whose combined, wider gaze acts as a flashlight making enemy action visible before it is too late to intervene.

The new approach offers open team and employee engagement as a method of implementing layered defenses, particularly on the front lines of detection and intervention, where critical operations take place.

The insider threat remains as alive as it is statistically rare, despite generations of study. Infiltrators continue to pose a risk to critical infrastructure and other institutions. There are no easy answers. No Dark Corners shows promise, however, as an approach to overcome gaps in traditional defenses. By going beyond corporate sentinels to engage stakeholders in their own protection, this approach offers the victory of ownership over surprise.

Future Research Needs

Just as Kelling's 1996 work on Broken Windows took experimental efforts in several municipalities to support the theory he and James Q. Wilson first espoused in 1982, No Dark Corners would benefit from the refinement and experiences that would follow implementing this model into one or more institutions. Such a project could involve the longitudinal study of a single organization to identify differences in susceptibility to insider threats before and after implementing the recommended innovations. Another variation would be to pilot a No Dark Corners implementation in one institution while comparing it to a sister organization or agency of comparable size and function where traditional methods remain in place. Results of this comparison could draw on a broad array of metrics, including measures of general productivity, positive or negative impacts attributed to insiders, and relative expenditure of resources for defense against such trust betrayers.

References

Akerstrom, M. (1990). *Betrayal and betrayers: The sociology of treachery.*

Allen, T. B., & Polmar, N. (1988). *Merchants of treason: America's secrets for sale.* NY: Delacorte Press.

Anderson, M. (1994). Introduction. In T. Sarbin, R. Carney, &. C. Eoyang (Eds.), Citizen Espionage: *Studies in Trust and Betrayal* (pp. 1–17). Westport, CT: Praeger.

Baker, S., Waterman, S., & Ivanov, G. (2010). In the crossfire: Critical infrastructure in the age of cyber war. Santa Clara, California: McAfee, Inc. Retrieved May 12, 2010 from *http://resources.mcafee.com/content/NACIPReport*

Band, S., Cappelli, D., Fischer, L., Moore, A., Shaw, E., & Trzeciak, R., Carnegie Mellon University Software Engineering Institute (2006). Comparing Insider IT Sabotage and Espionage: A Model-Based Analysis. PA: Carnegie Mellon University. Retrieved March 20, 2010 from *www.cert.org/archive/pdf/06tr026.pdf*

Ben-Yehuda, N. (2001). Betrayals and treason: *Violations of trust and loyalty.* Cambridge, MA: Westview.

Boveri, M. (1961). *Treason in the twentieth century.* (J. Steinberg, Trans.) London: MacDonald. (Original work published 1956.)

Brackney, R. C., & Anderson, R. H. (2004). *Understanding the insider threat.* Santa Monica, CA: RAND Corporation. Retrieved August 14, 2008 from *http://www.rand.org/pubs/conf_proceedings/CF196/index.html*

Bulloch, J. (1966). *Akin to treason.* London: Arthur Barker.

Cappelli, D.M., Moore, A.M., Trzeciak, R., & Shimeall, T.J. (2009). *Common Sense Guide to Prevention and Detection of Insider Threats. 3rd Edition– Version 3.1.* Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University.

Carney, R. M. (1994). The Enemy Within. In T. Sarbin, R. Carney, &. C. Eoyang (Eds.), *Citizen Espionage: Studies in trust and betrayal.* Westport, CT: Praeger.

Catrantzos, N. (2009). *No Dark Corners: Defending Against Insider Threats to Critical Infrastructure.* Master's thesis. Center for Homeland Defense and Security, Naval Postgraduate School, Monterey, California.

Cavelty, M.D. (2008). Like a phoenix from the ashes. In Cavelty, M.D., & Kristensen, K.S. (Eds.) (2008). *Securing the homeland: Critical infrastructure, risk and insecurity.* London; New York: Routledge.

Centre for the Protection of National Infrastructure. (2010). *Guide to Producing Operational Requirements for Security Measures.* London: CPNI.

Cherkashin, V. (2005). *Spy handler: The true story of the man who recruited Robert Hanssen and Aldrich Ames.* New York: Basic Books.

Covey, S. M. R., & Merrill, R. R. (2008). *The speed of trust: The one thing that changes everything.* New York: Free Press.

Department of Defense. (2000, April 24). *DoD insider threat mitigation: Final report of the insider threat integrated process team.* Retrieved August 18, 2008 from *https://acc.dau.mil/CommunityBrowser.aspx?id=37478*

Drucker, P. (2002). *Managing in the Next Society,* New York: Truman Talley Books.

Eoyang, C. (1994). Models of espionage. In T. Sarbin, R. Carney, &. C. Eoyang (Eds.), *Citizen Espionage: Studies in trust and betrayal* (pp. 69–91). Westport, CT: Praeger.

Fein, R., B., & Vossekuil, B. (1998). *Protective intelligence and threat assessment investigations.* Washington, DC: National Institute of Justice.

Fernandez-Araoz, C., Groysberg, B., & Nohria, N. (2009, May) The definitive guide to recruitment in good times and bad. *Harvard Business Review*, pp. 74–84.

Fishman, J. J. (2007). *The faithless fiduciary and the elusive quest for nonprofit accountability.* Durham, NC: Carolina Academic Press.

Garcia, J. (2009, September 21). Mitigating insider sabotage. SANS Institute InfoSec Reading Room.

Giesberg, J. (2001). The Role of Communication in Preventing Workplace Sabotage. *Journal of Applied Social Psychology,* 31:2439–2461.

Herley, C. (2009, September). So long, and no thanks for the externalities: The rational rejection of security advice by users. *Proceedings of the New Security Paradigms Workshop,* Oxford, United Kingdom. September 8–11, 2009.

Ho, S.M. (2009, August 6–9). Trustworthiness in virtual organizations. *Proceedings of the Fifteenth Americas Conference on Information Systems,* San Francisco, California.

Honnellio, A.L., & Rydell, S. (2007). Sabotage vulnerability of nuclear power plants. *International Journal of Nuclear Governance, Economy and Ecology,* 1:312–321.

ICE Mutual Agreement for Government and Employers. (2009, March 2). U.S. Immigrations and Customs Enforcement. Retrieved May 20, 2010 from *http://www.ice.gov/partners/opaimage/image_faq.htm*

Kaupla, J. (2008, May 25). Are you hiring future champions or future saboteurs? *ERE.net* (recruiters' network). Retrieved August 24, 2008 from *http://www.ere.net/2008/03/25/are-you-hiring-future-champions-or-future-saboteurs/*

Kelling, G. L., & Coles, C. M. (1996). *Fixing broken windows: Restoring order and reducing crime in our communities.* New York: Touchstone.

Kowalski, E., Cappelli, D., & Moore, A. (2008, January). *Insider threat study: Illicit cyber activity in the information technology and telecommunications sector.* Pittsburgh, PA: U.S. Secret Service and Carnegie Mellon Software Engineering Institute, pp. 24–26.

Leach, E.C. (2009). Mitigating Insider Sabotage and Espionage: A Review of the United States Air Force's Current Posture. Master's Thesis. Air Force Institute of Technology, Graduate School of Engineering and Management, Wright-Patterson Air Force Base, Ohio.

Leonard, D. & Swap, W. (2004, September). Deep smarts. *Harvard Business Review.* Retrieved July 29, 2008 from *http://harvardbusinessonline.hbsp.harvard.edu/hbsp/hbr/articles/article.jsp?ml_action=getarticle&articleID=R0409F&pageNumber=1&ml_subscriber=true&uid=24509483&aid=R0409F&rid=24600531&eom=1*

Masse, T., O'Neil, S., & Rollins, J. (2007). *The Department of Homeland Security's risk assessment methodology: Evolution, issues, and options for Congress* (CRS Report for Congress RL 33858). Retrieved August 16, 2008 from *https://www.hsdl.org/homesec/docs/crs/nps32-02070709.pdf&code=6a9f9433e059472a02fc2d35079cfc84* Washington DC: Congressional Research Service, pp. 5–9.

Murphy, P. (1999). *Surveillance. In Security business practices reference, Volume 2.* Alexandria, VA: ASIS International.

Newman, O. (1972). *Defensible space: Crime prevention through urban design.* New York: Macmillan Publishing Company.

Nieto, M., Johnston-Dodds, K., & Simmons, C. W. (2002). *Public and private applications of video surveillance and biometric technologies.* California Research Bureau. Sacramento: California State Library Foundation.

Noonan, T., & Archuleta, E. (2008, April 6). *The insider threat to critical infrastructures.* The National Infrastructure Advisory Council.

Olson, D. T. (2005). The path to terrorist violence: A threat assessment model for radical groups at risk of escalation to acts of terrorism. Masters thesis, Naval Postgraduate School, Monterey, CA. Retrieved September 5, 2008 from *https://www.hsdl.org/homesec/docs/theses/05Sep_Olson.pdf&code=08ed3b0e4d34e346e2dc3540cdc0e1f8*

Parker, J P., & Wiskoff, M.F. (1991). *Temperament constructs related to betrayal of trust.* Monterey, CA: Defense Personnel Security Research Center.

Peters, T. (2007, September 25). Speech on emerging security trends. Keynote address presented at the 2007 seminar and exhibits, ASIS International, Las Vegas, NV.

Puleo, A. J. (2006). Mitigating insider threat using human behavior influence models. Masters thesis, Air Force Institute of Technology, Wright-Patterson AFB, OH.

Shaw, E. D. & Fischer, L. F. (2005). *Ten tales of betrayal: The threat to corporate infrastructures*

by information technology insiders. Monterey, CA: Defense Personnel Security Research Center. Retrieved May 24, 2010 from *https://hsdl.org/?view&doc=86525&coll=public*

Shaw, E.D., Fischer, L.F., & Rose, A.E. (2009). *Insider risk evaluation and audit.* Technical Report 09–02. Monterey, CA: Defense Personnel Security Research Center.

Stein, J. (2010, May 23). The threat is real—Why aren't we worried? Book review: Cyber war by Richard Clark and Robert Knake. *Washington Post.* Retrieved May 23, 2010 from *http://www.washingtonpost.com/wp-dyn/content/article/2010/05/21/AR2010052101860.html*

U.S. Congress, Office of Technology Assessment. (1990, June). *Physical vulnerability of electric system to natural disasters and sabotage, OTA-E-453.* Washington, DC: U.S. Government Printing Office.

Vermeulen, F., Puranam, P., & Gulata, R. (2010 June). Change for change's sake. *Harvard Business Review,* pp. 71–76.

Wang, J., Hutchins, H.M., & Garavan, T.N. (2009). Exploring the strategic role of human resource development in organizational crisis management. *Human Resource Development Review,* 8:22–53.

Waters, T. J. (2006). *Class 11: Inside the CIA's first post-9/11 spy class.* New York: Dutton.

Weikel, D. (2008, September 5). LAX tightens security measures after alleged smuggling. *Los Angeles Times*. Retrieved September 5, 2008 from *http://mobile.latimes.com/detail.jsp?key=179165&full=1*

Wilson, J. Q., & Kelling, G. L. (1982, March). Fixing broken windows. *The Atlantic Monthly.*

Wright, P. Spycatcher: *The candid autobiography of a senior intelligence officer.* New York: Viking.

APPENDIX A: Checklist for Gauging Current Insider Defenses

Rating Scale: For each of these questions, rate your answer as High/hard, Medium, or Low/easy. Assign a score of 9 for High, 5 for Medium, and 1 for Low.

1. Thinking like an attacker, how difficult would it be for you to get the organization to hire someone who appears presentable, friendly, skillful, and has no identifiable history of criminal convictions or controversy. Assume an Internet search of social networking sites as something an employer will also check to uncover threatening activities.
2. Wander around physically and electronically (as via internal websites or network applications) through the organization. How difficult would it be for you to gain access to sensitive information that has nothing to do with your job, including the kind of detail that would help you pick a worthy target or help you determine how to destroy it?
3. How hard would it be for you to enter into or hide within an area where the most critical assets of the organization reside? Trying this after business hours or on a weekend, how hard is it to talk your way into high value or sensitive areas where you do not belong or do not have authorization to linger?
4. What is the extent to which you can expect team members at a critical area to spontaneously keep you out if you do not belong there or are not a member of that team?
5. How hard is it to get through your organization's probation period? (Consider asking around to see who can remember the last time someone was released during the probation period. If this is a routine occurrence, then the answer is High. If no one can remember the last time a new employee did not survive probation, the answer is Low.)
6. How much attention is paid to verifying identity for new hires? (Check this not by asking the department responsible for the checking but by finding recently hired employees and asking how carefully their identification was examined. If the process was a token effort that defaulted to the most junior clerk available, it rates Low. If there was careful scrutiny, it is High.)
7. What is the likelihood that if someone sees you doing something suspicious, threatening, or entirely out of place for the area, that person will approach you or report the matter so that there is immediate follow-up with you while you are still in the area?

Totals: Total your scores. If all are High, your total would be 70. If all Low, 7; and all Medium, 35.

55–70 Strong. There may be room for fine-tuning, but your organization is more resistant to hostile insiders than most, with good opportunities to detect or defeat the threat.

39–54 Above average. You have some defenses in place but probably need to bolster the ones that afford exploitable vulnerabilities.

7–35 Going through the motions. Your defenses are untested or more aspirational than substantive.

APPENDIX B: Steps to Introducing No Dark Corners at Work

1. **Think like an attacker, not like a defender.** Develop scenarios to test how hard it would be for you to penetrate your own organization.

2. **Plan for co-pilots in every critical cabin.** Using the co-pilot metaphor and starting with your critical areas, design them to operate with a level of transparency and mutual support that makes it virtually impossible for a single person to be running everything absolutely alone or without some level of co-worker oversight. Make it a team effort, not an inquisition.

3. **Resist the temptation to rely exclusively on specialists or monitoring technologies for your defense.** The goal is engagement at the team level. Promote taking a proprietary interest in not only the job but in the team, so that teams become self-weeding, self-policing, and mutually supportive.

4. **Thank and follow up.** In those situations where team members report suspicious activities to a corporate sentinel, always begin by expressing thanks and then give some timely feedback, even if all you can say is that you looked into the matter and found it innocuous.

5. **Limit invasive controls to those that count.** Don't alienate employees by burdening them with so many controls that it restricts their ability to do productive work. If you weed out bad performers early and foster cohesive, self-policing teams, you should be able to trust people who have worked into positions of responsibility. Maintain a sense of balance and give due attention to the core business without attempting to make every employee a snoop or sentinel.

6. **Evaluate your security procedures and abandon what is not working.** If your preemployment background investigation program is not screening out weak or problem employees, overhaul it. If you can't tell, start keeping track and gauging its results.

7. **Don't keep bad hires past the time it takes to spot them.** When in doubt, release a new hire from employment for any reason before probation is over.

8. **Use what you have.** Focus attention on a problem and results will follow. Use government-sponsored programs like ICE/IMAGE. At the very least, make sure your part of the organization follows security procedures. Often, there is a major disconnect between what is presumed or required to take place and what actually takes place.

APPENDIX C: Delphi Research and Applicability to Insider Threat

Why only 12 respondents instead of, say, 2,000?

The Delphi process is iterative yet anonymous, and required a significant commitment on the part of respondents, including responses that took the form of explanatory narratives. In order to obtain meaningful insights rather than just confirming the author's opinions, this study sought out practitioners who each have over 20 years of experience in responsible charge in their respective fields and were willing to voluntarily participate in what would otherwise constitute billable hours. This undertaking required the fullest stretch of the author's network and availing of professional courtesy. Despite 31 years of industry experience and an address book with some 2,024 entries, the author rated himself fortunate to be able to assemble a dozen professionals who contributed their career thoughts throughout the Delphi process.

Note that the Delphi method isolates respondents from each other, rather than gathering them together in a focus group. This technique defends against groupthink and offers equal deference to the introverted whose voices might otherwise go unheard in the presence of more vocal and extroverted participants gathered together in the same room.

In order to increase respondent numbers, the research would have risked a corresponding lowering of the bar in experience and insight of experts. Neophytes are in greater supply, as are graduate students who would be more receptive to providing iterative responses. However, such a response pool would necessarily rob the process of the kind of wisdom and "deep smarts" that come only through broad, practical experience over time (Leonard & Swap, 2004). In Delphi research, the smallest number of respondents should not fall under 10, hence this study settled on 12—in case of any losses from one round of questions to the next. In practice, informed analysts have gone on record to state that "the sample size varies… from 4 to 171 'experts.' One quickly concludes that there is no 'typical' Delphi; rather that the method is modified to suit the circumstances and research question (Skulmoski, G. J., Harman, F. T., & Krahn, J., 2007, p. 5)." Other analysts, applying the Delphi method to policy issues, found useful sample sizes varying from 10 to 50 experts (Linstone, H., & Turoff, M., 2002, p. 82).

The Delphi research effort itself extended from January through April 2009 and consisted of three iterative rounds of questions and feedback. Recruitment of experts and gathering of their signed, informed consent forms, in satisfaction of the requirements of the Institutional Review Board of the Naval Postgraduate School, took place between the months of November 2008 to January 2009.

What did the Delphi respondents represent?

The two tables on the following page give a fuller picture of respondent expertise without compromising identities.

Individual Expertise of Delphi Group Members

Expert 1	Case officer for two different U.S. government agencies. Recruited agents in foreign countries. Investigated fraud in private sector.
Expert 2	Chief executive and expert in uncovering collusive networks and in managing private sector collaboration with law enforcement and prosecuting agencies. Certified Protection Professional.
Expert 3	Senior investigator with global due diligence firms. Investigative journalist specializing in complex international fraud cases.
Expert 4	Ombudsman for major police force. Chief of detectives. Former military policeman.
Expert 5	Critical infrastructure security director. Former undercover agent of federal law enforcement agency. Certified Protection Professional.
Expert 6	Former case officer recruiting agents for U.S. in third world countries.
Expert 7	U.S. counterintelligence officer debriefing traitors.
Expert 8	Corporate executive and systems integrator for defense business formerly involved in development of intelligence platforms.
Expert 9	Career investigator, business owner specializing in uncovering complex corporate fraud.
Expert 10	Corporate executive, corporate communications specialist and crisis management adviser.
Expert 11	Critical infrastructure operations director involved in leading agency response to and recovery from major natural disaster.
Expert 12	Clinical psychologist specializing in workplace and domestic violence prevention, assessment, and response.

Composite Expertise of Delphi Group Members

Professional Expertise	Experts Possessing Expertise
Interaction with hostile people and organizations	12
Critical infrastructure protection, management	5
Corporate fraud investigations	5
Public or private sector undercover operations	4
Organizational response to international threats	4
Response to threats as a police or military professional	4
Workplace violence case management responsibility	4
Crisis communications and response	3
Executive with profit and loss responsibility	3

Recommended Reading

Leonard, D. & Swap, W. (2004, September) Deep smarts. *Harvard Business Review*. Retrieved July 29, 2008.

Linstone, H., & Turoff, M. (Eds.). (2002). The Delphi method: Techniques and applications. *New Jersey Institute of Technology.* Retrieved November 23, 2008.

Skulmoski, G. J., Harman, F. T., & Krahn, J. (2007). The Delphi method for graduate research. *Journal of Information Technology Education* (pdf), 6 . Retrieved November 23, 2008.

About the Author

Nick Catrantzos, CPP, currently manages security for a large public utility and critical infrastructure. In late 2009, he graduated from the Naval Postgraduate School's Homeland Security Master's program, where he won top writing honors for his thesis on the insider threat. Catrantzos previously directed operations for two international security consultancies, Control Risks and Kroll Associates, and led public sector vulnerability assessments under ManTech Security Technologies. As an intelligence collector, he was awarded the Meritorious Service Medal for outstanding service to two government agencies. Subsequently he safeguarded stealth technology in the defense industry.

Catrantzos first grew interested in the insider threat while managing intelligence exploitation of defectors at an overseas location. Subsequently, in the corporate arena during the closing days of the Cold War, he had occasion to manage business aspects of defense against hostile intelligence collectors and potential traitors seeking to clandestinely acquire the benefit of advanced American research and development. At Lockheed's headquarters he oversaw all background investigations into corporate employees and also co-managed institutional response to an international hostage situation involving staff trapped in a war zone. Later, he developed institutional policies and protocols for handling threats of workplace violence.

Catrantzos first began his involvement with infrastructure defense in 1996, when he briefed the then newly formed President's Commission on Critical Infrastructure Protection. He subsequently moved into private sector security and crisis management consulting, returning to concentrate on public sector vulnerabilities after the events of September 11, 2001.

The sole California representative to serve on three successive federal panels on drinking water infrastructure, Catrantzos was recognized in 2007 with the highest award of the Association of Metropolitan Water Agencies for dedication to security progress that "is a very significant contribution to water systems throughout the country."

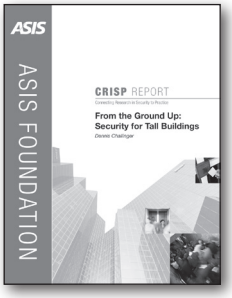
Catrantzos has contributed to two ASIS guidelines: *Facility Physical Security Measures and Workplace Violence*, and has contributed to *ASIS Security Business Practices Reference* Volumes 2, 3, 5, and 6.

Nick Catrantzos is a Certified Protection Professional and a licensed private investigator. He graduated magna cum laude with a baccalaureate in linguistics and summa cum laude with a master's in security studies with an emphasis in homeland security. He spent many years managing adverse consequences. Now he concentrates on preventing them.

He may be reached via *www.NoDarkCorners*.com, which links to his blog, *http://all-secure.blogspot.com*, where he discusses issues of the moment.

Additional CRISP Reports

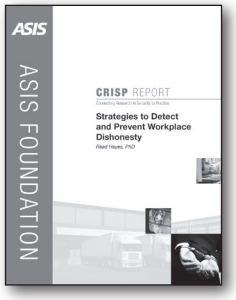
From the Ground Up: Security for Tall Buildings



Dennis Challinger

This report focuses on security challenges facing tall commercial and residential buildings. Challinger examines security threats, building vulnerabilities, and a variety of current responses. He also reports on research relating to the physical design of—and crime in—such buildings. His analyses lead to numerous research-justified recommendations.

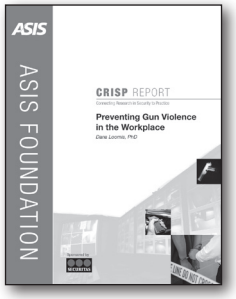
Strategies to Detect and Prevent Workplace Dishonesty



Read Hayes, PhD

Employee theft may account for 40-50 percent of all business losses. How can employers promote a culture of honesty? This report provides practical strategies to reduce workplace theft and fraud. Hayes examines the factors that lead to these behaviors; analyzes select prevention techniques, policies, and technologies; and offers research-based solutions.

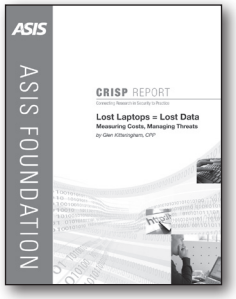
Preventing Gun Violence in the Workplace



Dana Loomis, PhD

New legislation may complicate your company's "no-weapons" policies. And there are many more potential perpetrators than just the usual suspects, from disgruntled former employees to domestic disturbances gone toxic. This report examines gun violence in the workplace and offers recommended approaches to prevent problems and minimize potential threats.

Lost Laptops=Lost Data: Measuring Costs, Managing Threats



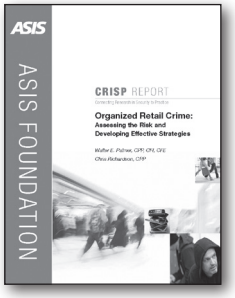
Glen Kitteringham, CPP

Replacing stolen laptops is just the start: lost productivity, damaged credibility, frayed customer relations, and heavy legal consequences can cripple your organization. This report reveals seven steps to protect laptops—and data—at the office, on the road, or at home. You get practical checklists and classification schemes to help determine adequate levels of data protection. Plus physical, electronic, and security measures you can immediately implement.

These reports are available as free downloads on the ASIS Foundation Web site, *www.asisfoundation.org*.

Additional CRISP Reports

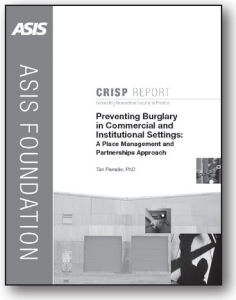
Organized Retail Crime: Assessing the Risk and Developing Effective Strategies



Walter E. Palmer, CPP, CFI, CFE
Chris Richardson, CPP

This CRISP report invites retailers to take a critical look at their handling of Organized Retail Crime (ORC). Chris Richardson and Walter Palmer combine their extensive experience of advising retailers on how to manage security risks with a very helpful summary of previous research, to stimulate thinking on how best to respond to ORC. Their starting point is that retailers and any others involved need to be clear about the type of ORC problem they are facing and its drivers, as well as the types of measures that are already in place that can be marshalled as part of an overall approach to making a response effective. They unpick the merits and limits of different types of security and offer a number of frameworks to guide practitioners. In so doing it is likely that this paper will become one of the essential reference points for those who need to tackle the ORC threat.

Preventing Burglary in Commercial and Institutional Settings: A Place Management and Partnerships Approach



Tim Prenzler, PhD

In this report Tim Prenzler, PhD, looks at how to assess, manage, and respond to burglaries that occur at commercial and industrial sites. While there is a considerable amount written about domestic burglary, research is less in evidence when the locale is non-residential. His report looks at the context in which burglaries occur, and includes a consideration of the burglar's approach. He examines a range of solutions, which aim to make it more difficult for would be offenders particularly in the workplace, and he shows where security managers can have an impact. Drawing together a range of data, he looks at approaches from different levels, from the police, the government, and from those closer to the offence, the "place managers." Those charged with preventing burglary at commercial and institutional settings now have a source of information, which connects research to practice to guide them in their prevention strategies.

These reports are available as free downloads
on the ASIS Foundation Web site, *www.asisfoundation.org*.

ASIS International (ASIS) is the preeminent organization for security professionals, with more than 37,000 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, government entities, and the 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*.

ASIS International Foundation

The ASIS Foundation, a 501(c)(3) nonprofit organization, advances the security profession worldwide by enabling leading-edge research, education, and training. Foundation awards and scholarships ensure those pursuing a security management career are able to realize their academic and professional goals. Support for the Foundation is achieved through financial contributions from individuals, chapters, and companies with an interest in the security industry. For details, visit www.asisfoundation.org.

ASIS FOUNDATION™

1625 Prince Street
Alexandria, VA 22314-2818
USA
+1.703.519.6200
Fax: +1.703.519.6299
www.asisonline.org

PLEASE PLACE BARCODE HERE
FOR ISBN # 978-1-934904-06-0