No Dark Corners: A Different Answer to Insider Threats

Nick Catrantzos

Everything we think we know about defeating the insider threat may not be wrong. It just fails to solve the problem. Background investigations are easily sidestepped. Institutional inquisitors – whether security staffs, auditors, cyber network custodians, or other corporate sentinels – repeatedly miss unmasking the infiltrator or saboteur until it is too late. Yet most organizations rely precisely on these sentinels as the first, last, and only line of defense. After all, it is their assigned job. At the same time, the sentinels' invasive audits and technical monitoring alienate essential employees while posing minimal hurdles to those whose aim is our ruin. Nevertheless, our institutions and received wisdom tell us to invest ever more resources in such defenses with dismal track records and unproven deterrent value. Might there be a better way?

THE PROBLEM

A 2008 report to the President explained the insider threat problem this way:

> 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.[1]

While reports such as these underscore the potential of insider threats, trust betrayal remains a statistically rare phenomenon.[2] If, as the literature suggests, a "miniscule fraction" of the people in a position to betray trust actually do so,[3] then quantitative methods offer limited value in uncovering practical countermeasures and strategic innovations. After all, if most people do not violate trust to the point of becoming a threat to their organization, statistical surveys of willing and benign respondents are unlikely to reveal telltale signs of trust betrayers. Under the circumstances, a qualitative approach may offer more insight into dealing with insider threats bent on visiting irreversible harm to American infrastructure and institutional targets. Accordingly, an application of the Delphi method offered a means of tapping the career experiences of a diverse group of experts in dealing with insider threats. The Delphi study results highlighted fissures in the fortress wall of existing countermeasures. Delphi study results also led to some innovations in defending against hostile insiders.[4]

DELPHI METHODOLOGY APPLIED TO INSIDER THREAT STUDY

For this research project on insider threats, the study asked seasoned defenders, investigators, and line managers to answer questions and distill judgments through the iterative Delphi research process.[5] This project consisted of recruiting a dozen experts from different organizations and disciplines and then asking them three series of questions over time. Respondents operated independently, with guarantees of

confidentiality, and without direct interaction with other experts. After the first round of questions, these respondents saw a compilation of all the answers to the first round and then addressed a second round of questions that were suggested by the first. Similarly, for the third and final Delphi round, respondents saw 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 have claimed, "we need multidisciplinary research teams (not just *geeks*) investigating what we should look for as indicators of possibly malevolent behavior."[6]

The group of experts in this study consisted of a dozen professionals representing different disciplines, such as counter espionage, prevention of workplace violence, defense against systemic institutional fraud, corporate response to handling reputational risk, as well as law enforcement, military, and business profit-and-loss experience. Each respondent possessed at least twenty years of professional experience and first-hand exposure to managing or investigating insider threats. Each Delphi round involved transmitting questions by e-mail, with responses returned via e-mail, with at least two weeks between rounds. All respondents agreed to participate in the study under standard confidentiality protections and with repeated reminders that no classified or proprietary information was being solicited for the study. Of the dozen experts who agreed to participate in three rounds of Delphi surveys, 100 percent saw the process through from start to finish, from January to April, 2009.[7] Initially, Delphi experts suggested that traditional countermeasures, such as random audits, would stand fast between a hostile insider and a devastating attack. However, by the time the same experts were induced to trade places and evaluate their own countermeasures in terms of how they would impede the experts themselves from carrying out a successful insider attack, the story had changed dramatically.

Initially, the hostile insider seemed likely to emerge as a disgruntled employee with the capacity to plan a devastating attack and the arcane knowledge to make the most of the opportunity.[8] Indicators of this trust betrayer included unexplained anger and other suspicious behaviors, like undue secrecy and self-aggrandizement, potentially serving as red flags. Finally, countermeasures such as random audits, monitoring of employees, and investigations appeared likely to offer value as ways to thwart this kind of insider. By the end of the Delphi process, however, the same experts arrived at different conclusions. Their judgments flew in the face of this accepted wisdom. Despite being unable to see each other's observations or remarks, the Delphi experts ultimately converged on findings that ran counter to their own initial assumptions and to the accepted wisdom on insider threat defense.

COUNTERINTUITIVE FINDINGS

Infiltrators More Likely Threat than Disgruntled Insiders

Research results suggested that the terrorist attacker targeting institutions such as stewards of critical infrastructure would more likely use an infiltrator than a disgruntled insider already in place.[9] A career employee with long-term access and in-depth knowledge of inner workings will necessarily know more about how to dismantle the organization or its critical assets than an infiltrator new to the entity. The same careerist, given time and inclination to plan, 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 egocentric to accept direction readily Volatility makes this person an operational risk who may compromise details of an attack out of disagreement with the particulars or out of spite at not being consulted on every move. [10]

Additionally, in the age of the Internet and with critical infrastructure targets that have traditionally operated openly without the security precautions of the national security sector, targets and their employees remain highly accessible. Their critical assets are often immobile. Thus, in contrast to weapons classified for reasons of national security, critical infrastructure cannot be relocated or concealed once its location and operating details have been compromised. In this context, the targeting information necessary for mounting an infrastructure 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 to enable an attack without having to spend years masquerading as an innocuous employee. We also need to remember that many infrastructures and institutions are desperate for talent and have aging work forces with few systemic arrangements for recruiting, training, and deploying successors. Thus, as one expert noted, infrastructure employers are prone to welcome any 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 unfettered 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 influencing the possibility of another. In this milieu, if the remaining defenses (described below) 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 he can definitely be better controlled, focused, and more disciplined about concealing telltale indicators of an impending attack to avoid compromising the attack.

Weakness of Traditional Defenses

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.[11]

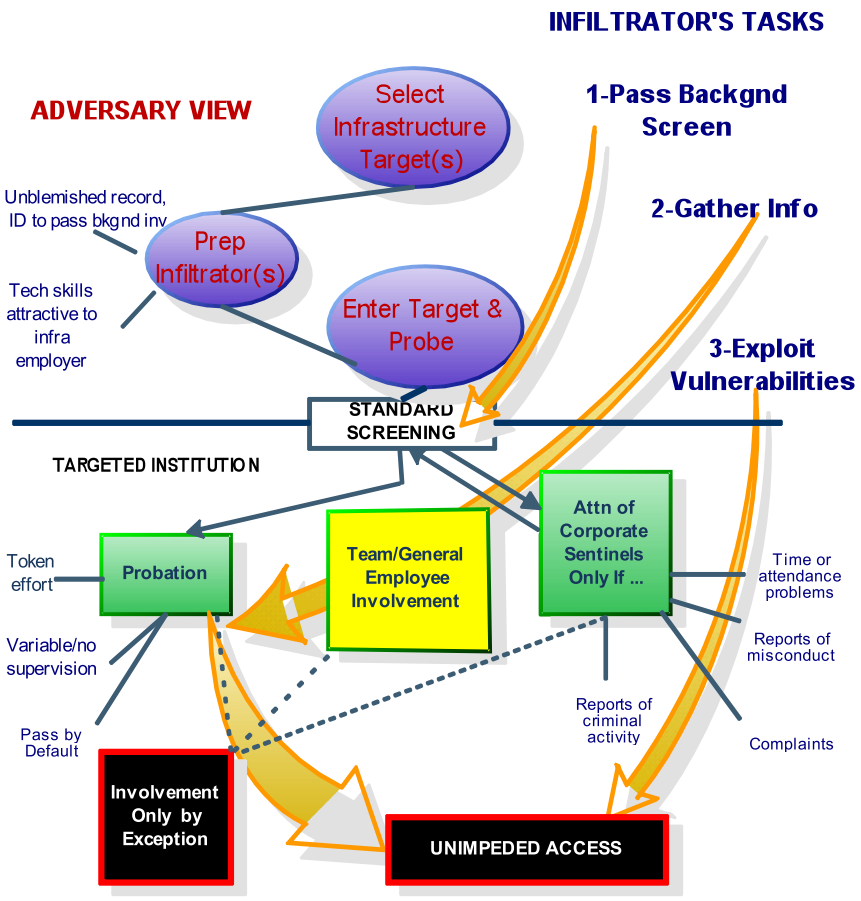

Figure 1. Traditional Situation: Infiltrator Meets Infrastructure

Figure 1 depicts the situation in which infiltrator and infrastructure 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 during which, or at least after which, the infiltrator anticipates having sufficient freedom of maneuver to gather information unimpeded by any close scrutiny or interference. The infiltrator eluding detection or interference is free to operate in the dark corners of insufficient oversight and management, 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 permitted for national security employment are not available for the public and private sector employers who operate 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.[12] However, as Herbig 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.[13] Consequently, yesterday's focus on finances as an indicator of possible trust betrayal offers limited value in detecting today's traitors who will be living well within their means. They will also be showing no signs of the kind of debt indicative of financial hardship that would make them targets for bribery or ostensible candidates for selling out their employers to relieve financial distress.

Similarly, an infiltrator sent into an infrastructure employer 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 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.[14] 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 infrastructure 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. Moreover, the larger and more sophisticated the attacker's organization, the more candidates 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 America 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.[15] 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."[16] 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 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. In the broader context of employment law, anti-discrimination protections, and limitations on the extent to which employers may practically scrutinize applicants for work at critical infrastructure sites, 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.[17] Like pre-employment 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 would have aged enough to cast doubt on his or her motivational zeal and to be suspected of beginning to identify too closely with the target.

2. 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, rarely interact with the new employee. They may participate in a new-hire orientation, but otherwise they deal with the newcomer only if the latter's actions or questions affect their various disciplines. The new employee benefits from a grace period during which minor transgressions committed in the course of gathering information are easily dismissed as a rookie's excusable faux pas. Unless the neophyte does something egregious to excite remark, he or she is unlikely to face a random audit or active monitoring of computer key strokes, or time and duration of access into a given work space. On the rare occasion when an infiltrator's actions invite challenge, all that are necessary to deflect focused attention of corporate sentinels are 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 note that so-called random audits are seldom truly random. As one of the experts pointed out, the astute observer sees them coming. Moreover, many audits are perfunctory, particularly if auditors consider themselves overextended and loathe taking 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."[18] This explains why a resource-intensive audit will not be "wasted" on a neophyte who has still not even passed probation.

In many, if not most critical infrastructure environments, audits are by definition adversarial. They are, therefore, regarded as a necessary evil perpetrated by individuals who are more tolerated than esteemed. To the extent that auditors are aloof, disdainful, or menacing, they struggle to obtain active cooperation. One Delphi expert has seen 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 is 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 no threat to the infiltrator operating with a modicum 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.

First, for every device capable of tracking activity, there must exist somewhere in the institution a means of discriminating untoward 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 exceed the capacity of the average financially-strapped 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 snooping by a designated monitoring force. Delphi experts 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.

Thwarting such corporate sentinels, whether human overseers or automated devices, soon becomes part game, part badge of honor. Operators then 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.

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."[19]

In this context, the institution comes to rely excessively on its corporate sentinels, viz. its designated watchers, such as security staff, leaving the rest of the workforce indifferent to a defensive role that the employees and managers leave to such specialists. Meanwhile, the capacity of these sentinels, to focus limited resources on discovering a needle-in-the-haystack level of visibility of an insider threat is constrained by infrastructure operator resistance to draconian security measures that are too 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.

ALTERNATIVE: NO DARK CORNERS APPROACH

One way to overcome the vulnerabilities in the foregoing defensive measures is to re-examine Figure 1'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.

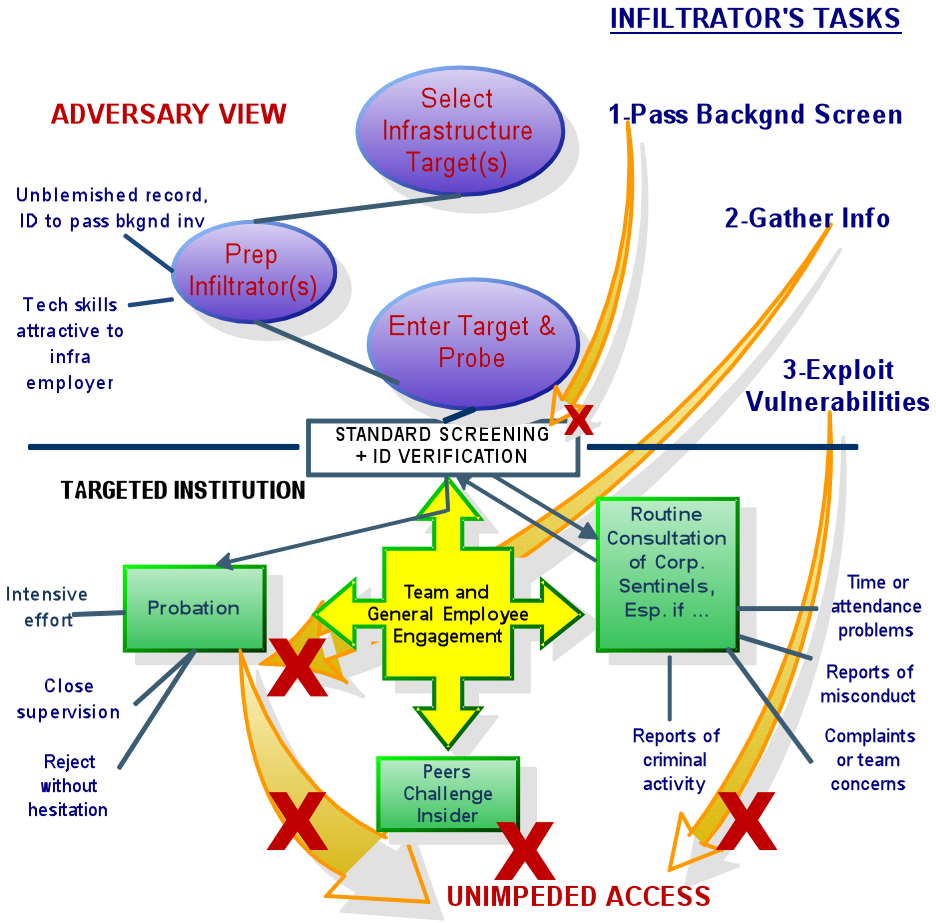

Figure 2. Desired End-State for Infrastructure vs. Hostile Insider

What has changed? First, the screening process no longer relies excessively on a search for indicators that uncover neither an infiltrator nor other hostile insider. As one executive who studied trust betrayal for an entire career pointed out, many experts find that personnel investigations do not prevent espionage or detect those who may commit such a crime.[20] 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,[21] infrastructure 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 via a federally-funded program that trains human resources recruiters to check credentials and gives access to Social Security and immigration databases to facilitate verification of employment eligibility.[22]

The new screening program will not necessarily catch all infiltrators any more than it will defeat individuals who enter the institution benevolently and only later develop hostility and a propensity to betray or destroy. However, the program will reduce the ability of terrorist organizations to infiltrate their agents with falsified credentials which, absent increased scrutiny, receive only token examination from the most junior clerk assigned to processing employment applications. This is why Figure 2 shows a smaller X next to the arrow depicting the infiltrator's first task. The new screening program complicates 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 now support the screening process by at least 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 employment unless they demonstrate talent worth keeping. This demonstration must satisfy not only the supervisor but teammates as well, which forces close interaction on a daily basis. 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. This approach eliminates 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 breathes life into this security prescription of management expert Tom Peters when exhorting security professionals 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. [23]

At the heart of the cultural shift, this alternative approach also increases the opportunity to detect any insider threat because it spreads defensive responsibility pervasively, rather than relying exclusively on corporate sentinels.

BALANCING TRUST AND TRANSPARENCY: THE CO-PILOT MODEL

How can a cultural shift in the workplace create a team whose members constantly monitor each other without undermining the trust necessary for internal cohesion? On the surface, it would appear that such a team is merely relieving assigned corporate sentinels of their snooping 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.[24] Extending the pilot and cockpit metaphor from the preceding discussion on employment probation periods, however, offers an answer to this apparent contradiction.

In line with the cultural shift to internal team monitoring, every team member becomes not an inquisitor but a co-pilot. The key elements of the co-pilot definition that apply are of a "qualified pilot who assists or relieves the pilot but is not in command."[25] The co-pilot has 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. Neither a co-pilot nor a team member need become a snoop or tattletale. Yet both 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.[26]

While many parts of a given countermeasure carry forward into the new framework, the means of applying the countermeasure changes fundamentally. No Dark Corners transforms invasive techniques into performance gauges for work teams. A video camera monitoring a critical process involving hazardous materials should now be welcome as a way for a fellow team member to be able to summon assistance if another team member in the area gets hurt – not as a spy camera for helping bosses catch subordinates in the act of violating established procedures. The same cultural shift should make team members appreciate having a back-up control room operator or lineman within earshot or line of sight, rather than bristle at the thought of not being trusted to work alone. Embracing the co-pilot model should transform additional physical or electronic monitoring into a welcome means of summoning assistance. It should also limit opportunities for a hostile insider to act against the institution. Ultimately, greater transparency and work redesign should limit opportunities for clandestine and damaging activities by eliminating the dark corners that insider threats need to do their worst.

CONTRAST WITH TRADITIONAL APPROACH

Applying the No Dark Corners 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 of these watchers to monitor every process or venue. By contrast, in a No Dark Corners arena, the one who may be watching is a co-worker who has a proprietary interest in the institution and will therefore act to defend it.

Figure 3 highlights key features of this strategy, showing innovations, as well as what management authority Peter Drucker emphasized as a primary duty of all organizations: organized abandonment of processes and strategies that are no longer working.[27] A method of fostering the creation of innovative strategies according to some observers, this grid challenges the institution to act on four key features in order to arrive at meaningful innovation.[28]

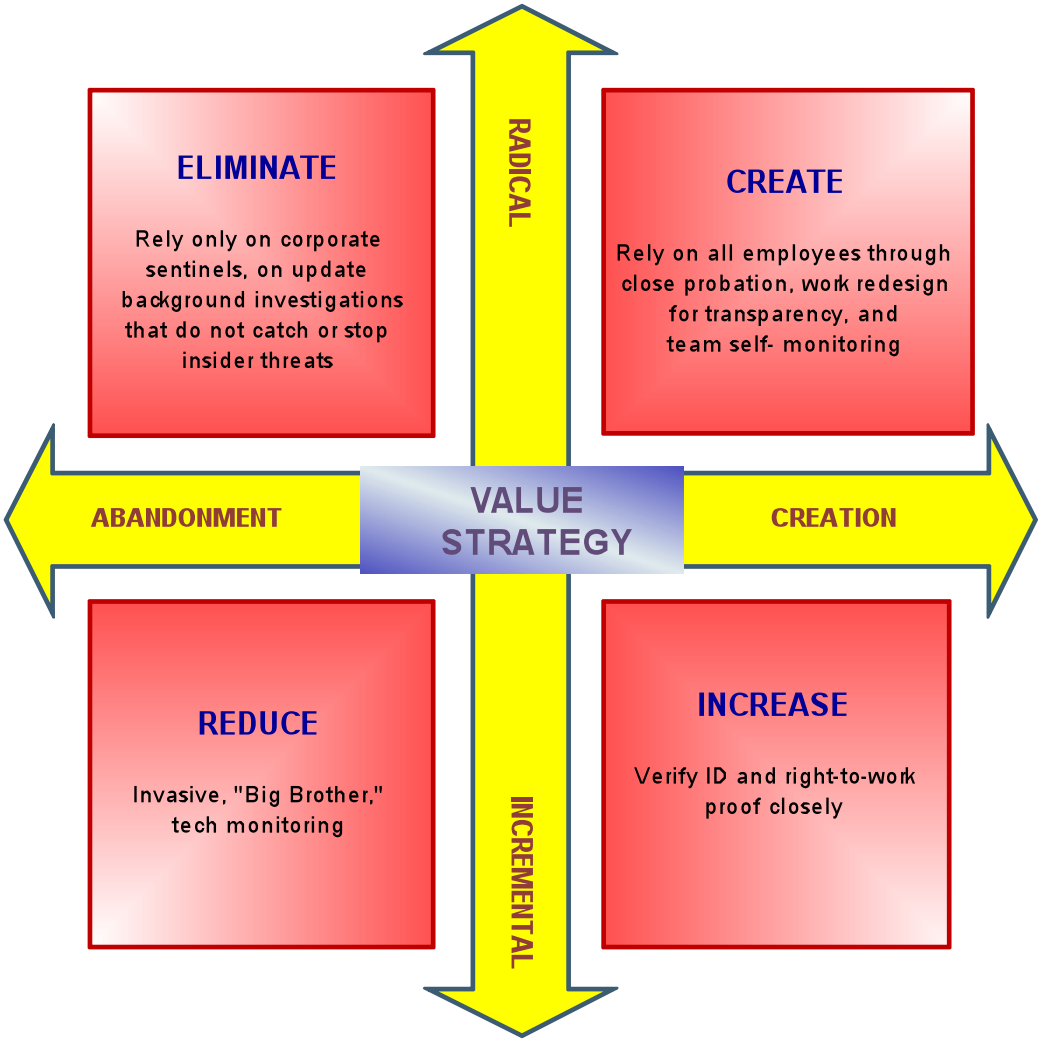

Figure 3. Key Features of No Dark Corners Strategy[29]

As Figure 3 shows, measures that impede an infiltrator's ability to surveil or strike take precedence over measures that are easily bypassed and 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 No Dark Corners approach. Figure 4 presents this contrast in the form of a strategy canvas where the status quo appears in red and a breakaway challenge to this strategy, i.e., No Dark Corners, appears in blue.

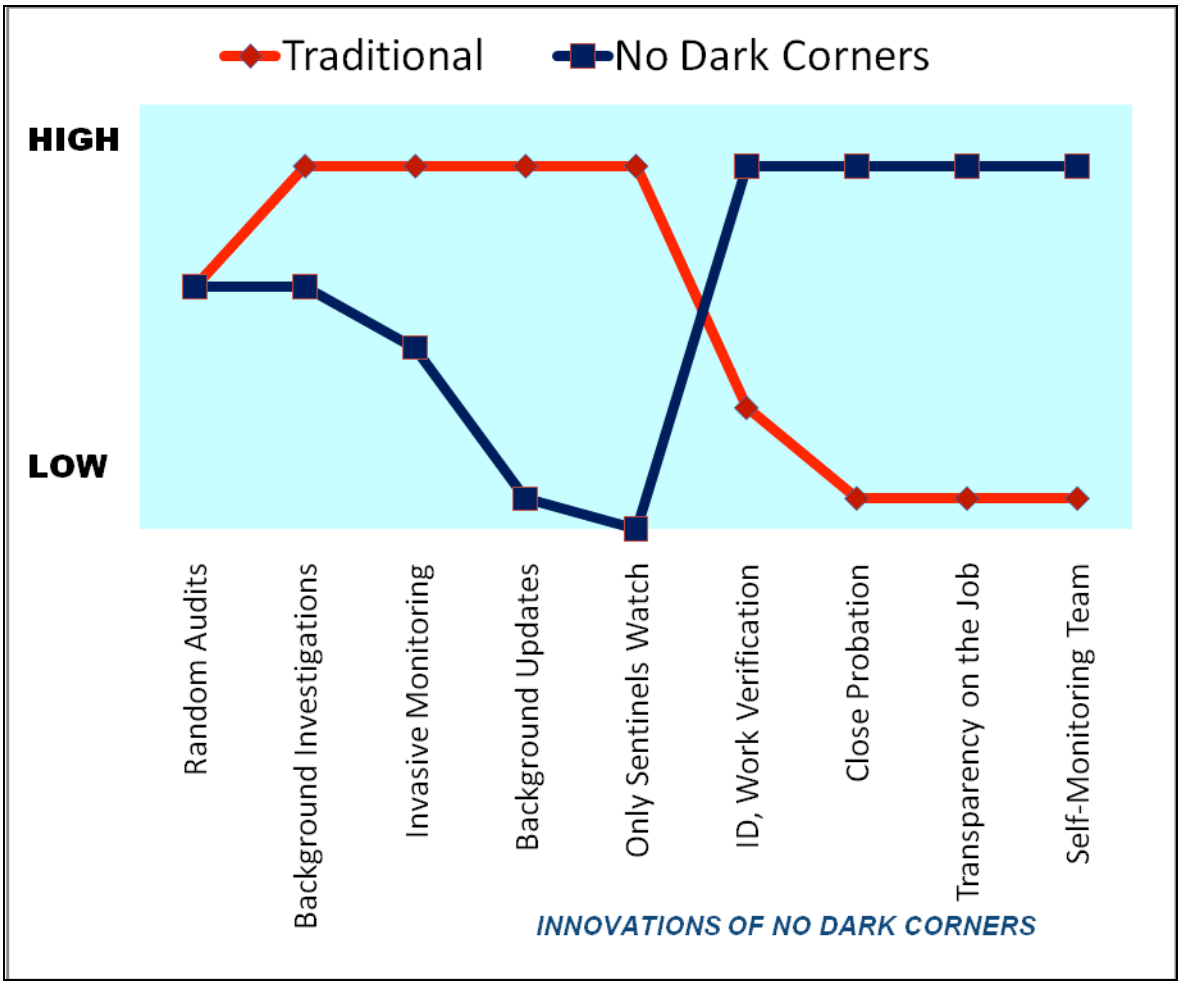

Figure 4. Strategy Canvas: Traditional vs. No Dark Corners

The strategy canvas is at once a gauge and a framework for revealing where traditional insider defenses have faltered and where the innovations of No Dark Corners offer alternatives to reduce chronic vulnerabilities. The canvas visually communicates the current state of affairs in insider threat defense (in red) while also showing the potential for breaking new ground (in blue) to reduce susceptibility to infiltrators and, by extension, to any hostile insider.

In addition to adjusting defensive measures already discussed at length throughout these pages, Figure 4 draws attention to three particular innovations that reflected insights both of Delphi experts 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 value, as well as defensive benefits.

Close Probation

As one study shows in extolling the virtues of close probation for example, "organizations that systematically integrate new employees enjoy lower turnover, and the recruits report greater commitment and job satisfaction."[30] This and the other tools intend to defeat hostile insiders through the kind of scrutiny that corporate sentinels cannot match, namely, the scrutiny of a co-worker, or what one analyst calls a "citizen-sentry." [31]

In critical infrastructure institutions, probationary periods are the ideal means of rejecting a new hire for any reason, without having to meet the rigors of bargaining unit constraints that are the equivalent of academic protections for tenured professors. Yet, Delphi-respondent experience shows that two parts of the probation process are under-exploited. Hiring managers hesitate to release probationary employees, particularly if the internal hiring process is lengthy, complicated, and demanding of management time. To make matters worse, in many cases, the longer a vacancy goes unfilled, the greater the chance of losing that position, as upper management can see that work goes on despite the vacancy. Finally, in areas where supervision is traditionally lax, mentoring and monitoring of probationary employees is absent, thereby predisposing hiring managers to keep the probationary employee by default.

In reversal of this process, No Dark Corners puts a premium on using the probation period as a line of institutional and infrastructure defense. The default shifts away from keeping the new hire absent overwhelming evidence of a problem. Instead, the default becomes termination at the first sign of any problem and automatic release at the end of probation absent ostensible proof that the new employee adds value. The only way for this proof to surface is through close supervision, which means active engagement of front-line supervisors and fellow members of a work team. The supervisor acts as the pilot, with the rest of the team members 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 strategy 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 environments,[32] every job and work space should be designed to maximize visibility to peers and minimize opportunities for clandestine, hostile action. 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 attivities 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.[33] Process-monitoring cameras, which assist with environmental watching of systems to be sure 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.[34] 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 in the course of routinely looking out for each other.

Team Self-Monitoring

Finally, No Dark Corners recognizes and seeks to exploit the difference between over-the-shoulder audits and self-policing out of work team cohesion and pride. As a Delphi expert 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.

As another Delphi expert 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 found that 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. An expert reasoned that this kind of self-monitoring, properly encouraged and applied to defense against insider threats, would present an almost insurmountable obstacle to infiltrators intent on an attack against critical infrastructure.

NO DARK CORNERS LINKAGE TO OTHER SECURITY STRATEGIES

The No Dark Corners 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 or activity to exercise a proprietary interest sufficient to defeat adversary encroachment. In his seminal work, 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."[35]

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 twenty years, despite considerable investment.[36]

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.[37] 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.[38] Soon, vandals break all the remaining windows. 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 defended areas.[39]

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, No Dark Corners adds private space into the mix, as all critical infrastructures have control rooms and physical assets that are not open to the public, hence, out of the public view. Invariably, however, critical infrastructures also include important assets that are exposed to public view, such as transmission lines and aqueducts, which may be visible or accessible to members of the public.

Why has this not happened before? Because infrastructure defense is assumed to fall primarily into the hands of the private sector.[40] By extension, the critical assets must, therefore, be under private control and not in the kinds of public spaces where there apply existing models of defense through a sense of ownership, like Defensible Space and Broken Windows theories. The reality, however, is that critical infrastructure may be impossible to secure in some cases, as in transmission lines, aqueducts, and fiber-optic cables stretching across broad expanses of undefended territory.

No Dark Corners reduces relatively unproductive but resource-intensive investment in countermeasures that an infiltrator can readily bypass. The strategy shifts exclusive reliance of institutions on overly specialized monitors, the 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 pre-employment background investigations and unproductive update investigations, which may deter obvious criminals but will not defeat a hostile infiltrator.[41] 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 close the door to a major penetration vulnerability in the hiring process.

At the same time, 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.

Envisioning a No Dark Corners Workplace

In a No Dark Corners workplace, standard screening will have new emphasis on identity and right-to-work verification, and false credentials will be subject to discovery, making it particularly difficult for a foreign adversary to penetrate an American institution. Close probation means an infiltrator will face unabated 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 unrelated to the individual job and breaching protocols under the banners of ignorance or deficient supervision. Corporate sentinels previously mistrusted will be accessible to team members to follow up on their concerns and suspicions. In the process, the sentinels themselves will 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.

Limitations and Opportunities for Further Research

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 awaits the refinement and validation that would follow introduction of this model into an institution. Ideally, such an institution could be compared to a sister organization or agency of comparable size and function. Results of this comparison would 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 adversaries. Alternatively, a single institution adopting the No Dark Corners strategy could compare itself across a similar scale to determine the impact of the new strategy in relation to previous experiences with insider problems under alternative defensive strategies.

CONCLUSION

As this study suggests, a hostile insider needs three essentials to carry out an attack: a worthy target, an open door, and a dark corner. Any adversary seeking to strike a devastating blow against any institution needs the same.

Level 1, or primary, critical infrastructures, such as power, water, and telecommunications make worthy targets. Not only are some of them irreplaceable, their damage or destruction leads to cascading failure of other, interdependent infrastructure components, from banking and finance to emergency responders, from transportation and logistics to food and agriculture. All depend on the Level 1 infrastructures – on worthy targets.

The open door comes from a traditional culture of unrestricted public access. This openness flourishes because public and investor-owned utilities must answer to a demanding public, ratepayers, and various regulatory agencies. Even when these infrastructure stewards 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.

Even if an infiltrator sets sights on a worthy infrastructure target and exploits weak defenses, he or she still needs a dark corner free of oversight or restraint 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.

Second, as previously mentioned, Americans have a penchant for relying on technology to solve problems. This tendency places a premium on depth at the occasional expense of breadth. As a result, in addressing the insider threat to critical infrastructure, the tendency leaves us attempting to penetrate with the intensity and focus of a laser what we should 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 impunity.

The No Dark Corners approach substitutes the flashlight of open team and employee engagement for the laser of limited and specialized monitoring of corporate sentinels working in secret. It represents a method of implementing layered defenses, particularly on the front lines of detection and intervention: where critical operations take place.

Despite generations of study, the insider threat remains alive. Infiltrators continue to pose a risk to critical infrastructure. There are no easy answers. No Dark Corners shows promise, however, as an approach that fills the gaps in traditional defenses. In so doing, this approach stands poised to deliver an important benefit for defenders: the victory of ownership over surprise.

Nick Catrantzos manages security for a large public steward of critical infrastructure. The sole California representative to serve on three successive federal panels on drinking water infrastructure, Catrantzos was recognized in 2007 with the Donald R. Boyd Award of the Association of Metropolitan Water Agencies for dedication to measure security progress in the water sector that "is a very significant contribution to water systems throughout the country." Catrantzos holds a master's degree from the Naval Postgraduate School Center for Homeland Defense and Security, where he received the outstanding thesis award. Catrantzos once worked for a discreet arm of public service, and has divided thirty years of intelligence and security experience between the public and private sectors. 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 moment.

---

[1] T. Noonan and E. Archuleta, *The Insider Threat to Critical Infrastructures* (The National Infrastructure Advisory Council, April 6, 2008), 32.

[2] E. D. Shaw and L. F. Fischer, *Ten Tales of Betrayal: The Threat to Corporate Infrastructures by Information Technology Insider* (Monterey, CA: Defense Personnel Security Research Center, 2005),

https://www.hsdl.org/homesec/docs/dod/nps33-122107-01.pdf&code=cabcfb03c46e06e36ad177e692594c28.

[3] C. Eoyang, "Models of Espionage," in *Citizen Espionage: Studies in Trust and Betrayal*, ed. T. Sarbin, R. Carney, and C. Eoyang (Westport, CT: Praeger, 1994), 80.

[4] N. Catrantzos, "No Dark Corners: Defending Against Insider Threats to Critical Infrastructure" (master's thesis, Center for Homeland Defense and Security, Naval Postgraduate School, Monterey, California, September 2009), https://www.chds.us/?research/thesis&view=public.

[5] G. J. Skulmoski, F. T. Harman, and J. Krahn, "The Delphi Method for Graduate Research," *Journal of Information Technology Education* 6 (2007), http://jite.org/documents/Vol6/JITEv6p001-021Skulmoski212.pdf

[6] R. C. Brackney and R. H. Anderson, *Understanding the Insider Threat* (Santa Monica, CA: RAND Corporation, 2004), 14, http://www.rand.org/pubs/conf_proceedings/CF196/index.html.

[7] Catrantzos, "Dark Corners," 6-10.

[8] Ibid., 5-38.

[9] Ibid., 11-41.

[10] Ibid., 26.

[11] Ibid., 43-50.

[12] T. B. Allen and N. Polmar, *Merchants of Treason: America's Secrets for Sale* (New York: Delacorte Press, 1988), 3 and 47.

[13] K. L. Herbig, "Changes in Espionage by Americans: 1947–2007," *Technical Report 08–05* (Monterey, California: Defense Personnel Security Research Center, March 2008), V.

[14] 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, *Pre-employment Background Screening Guideline* (Alexandria, Virginia: American Society for Industrial Security, International, 2006), http://www.asisonline.org/guidelines/guidelinespre-employ.pdf.

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

[16] *Pre-employment Background Screening Guideline*, 24.

[17] Ibid., 20 and 22.

[18] J. J. Fishman, *The Faithless Fiduciary and the Elusive Quest for Nonprofit Accountability* (Durham, NC: Carolina Academic Press, 2007), 274.

[19] R. M. Carney, "The Enemy Within," in *Citizen Espionage: Studies in Trust and Betrayal*, ed. T. Sarbin, R. Carney, and C. Eoyang (Westport, CT: Praeger, 1994), 21.

[20] M. Anderson, "Introduction," in *Citizen Espionage: Studies in Trust and Betrayal*, ed. T. Sarbin, R. Carney, and C. Eoyang (Westport, CT: Praeger, 1994), 1-17.

[21] 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 (*Pre-employment Background Screening Guideline*, 20, 22).

[22] *ICE Mutual Agreement for Government and Employers* (U.S. Immigrations and Customs Enforcement, March 2, 2009), http://www.ice.gov/partners/opaimage/image_faq.htm.

[23] T. Peters, speech on emerging security trends. Keynote address presented at the 2007 seminar and exhibits, American Society for Industrial Security, Las Vegas, NV, September 25, 2007.

[24] S. M. R. Covey and R. R. Merrill, *The Speed of Trust: The One Thing that Changes Everything* (New York: Free Press, 2008), 292.

[25] *Merriam Webster Dictionary Online* (2009), http://www.merriam-webster.com/dictionary/co-pilot.

[26] See Appendix D, items 1, 2, and 5, in Catrantzos, "No Dark Corners," for Delphi respondent illustrations of this point.

[27] P. Drucker, *Managing in the Next Society* (New York: Truman Talley Books, 2002), 295.

[28] W. C. Kim and R. Mauborgne, *Blue Ocean Strategy* (Boston, MA: Harvard Business School Press, 2005), 27-35.

[29] See Catrantzos, "Dark Corners," 55-56

[30] C. Fernandez-Araoz, B. Groysberg, and N. Nohria, "The Definitive Guide to Recruitment in Good Times and Bad," *Harvard Business Review* (May, 2009), 74–84.

[31] Fishman, *The Faithless Fiduciary,* 311.

[32] See Appendix D, item 2, in Catrantzos, "No Dark Corners," for more detail on the two-person integrity rule.

[33] For representative observations supporting the merits of such video surveillance, refer to M. Nieto, K. Johnston-Dodds, and C. W. Simmons, *Public and Private Applications of Video Surveillance and Biometric Technologies* (California Research Bureau. Sacramento: California State Library Foundation, 2002), 34, and P. Murphy, "Surveillance," *Security Business Practices Reference, Volume 2* (Alexandria, VA: American Society for Industrial Security, 1999), 19. Patrick Murphy, Loss Prevention Director for Marriott International, confirmed experiencing an 84 percent 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 a best industry practice in 1999 and which still holds true ten years later (personal communication, July 23, 2009).

[34] Nieto, Johnston-Dodds, and Simmons, *Public and Private Applications*, 16, and R. Day, "Remotely Monitored CCTV Reduces Theft by 80%," in *Secure Times (*Essex, UK: Sheen Publishing, Ltd., May, 2009), 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 percent as of June 2009.

[35] O. Newman, *Defensible Space: Crime Prevention through Urban Design* (New York: Macmillan Publishing Company, 1972), 6.

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

[37] J. Q. Wilson and G. L. Kelling, "Fixing Broken Windows," *The Atlantic Monthly,* March, 1982.

[38] G.L. Kelling and C.M. Coles, *Fixing Broken Windows: Restoring Order and Reducing Crime in Our Communities* (New York: Touchstone, 1996), vx.

[39] 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 legitimate users of the public away, 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, thus bringing into question Broken Windows as a panacea. One criticism even went so far as to opine that greater access of unwed mothers to abortion should account for crime reduction because children who would have grown to be criminals were aborted, and Kelling did not credit this phenomenon in his theory [S. D. Levitt and S. J. Dubner, *Freakonomics: A Rogue Economist Explores the Hidden Side of Everything* (New York, NY: HarperCollins, 2005)]. 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 in terms of actual aims and results. More recent criticisms focus on community policing aspects of the theory, which vary greatly depending on the police force. However, researchers Braga and Bond highlighted this point but 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,

http://www.boston.com/news/local/massachusetts/articles/2009/02/08/breakthrough_on_broken_windows/?page=2).

[40] R.T. Marsh, Chairman, President's Commission on Critical Infrastructure Protection, in cover letter to the president dated October 13, 1997, *Critical Foundations – Protecting America's Infrastructures: The Report of the President's Commission on Critical Infrastructure Protection* (Washington, DC: U.S. Government Printing Office, October 1997), http://www.fas.org/sgp/library/pccip.pdf. As Marsh noted, "Because the infrastructures are mainly privately owned and operated, we concluded that critical infrastructure assurance is a shared responsibility of the public and private sectors."

[41] Basic pre-employment 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 will in some measure depend on having a history free of criminal convictions and otherwise free of easily identifiable discrepancies that background checks are designed to spot.