2018-06

Insider Threat: Applying No Dark Corners Defenses

Catrantzos, Nick

Catrantzos N. (2018) Insider Threat: Applying No Dark Corners Defenses. In: Masys A. (eds) Handbook of Security Science. Springer, Cham; DOI https://doi.org/10.1007/978-3-319-51761-2_7
http://hdl.handle.net/10945/59238

Insider Threat: Applying No Dark Corners Defenses

Nick Catrantzos

Contents

N. Catrantzos (✉)
Center for Homeland Defense and Security, Naval Postgraduate School, Monterey, CA, USA
e-mail: NickHSx@gmail.com

A. J. Masys (ed.), *Handbook of Security Science*,
https://doi.org/10.1007/978-3-319-51761-2_7-1

Abstract

Unlike a frontal attack, an insider threat is a menace that operates from within established defenses and also possesses legitimate access to targets. Insider threat studies draw from many disciplines, with cyber-centric studies currently dominating the field. All disciplines hew to the convention of over-relying on experts and imposing heavy burdens on employees who pose no threat. One possible rationale is that experts see the insider threat as a problem when it is a predicament requiring a higher level of interpretive thinking to address.

Contrary to accepted wisdom, the No Dark Corners approach places monitoring responsibility at the co-worker level, rather than in the exclusive hands of experts, and broadly fosters an environment of transparency where co-workers function as copilots who take an active hand in their own protection. The ultimate aim is denying hostile insiders the opportunity to inflict harm by eliminating their ability to exploit institutional vulnerabilities that represent the dark corners from which an adversary needs to operate in order to penetrate and strike the targeted organization.

A strategy canvas depicts the contrasts between the conventional approach and No Dark Corners. The role of some other prominent aspects of insider threats and defenses is also discussed, including deception, knowledgeable escort, lawful disruption, and the curse of the indelicate obvious. Some societal implications and applications are also explored in broad strokes.

Keywords

Insider threat · No Dark Corners · Predicament · Copilot · Background investigations · Random audits · Lawful disruption · Deception · Curse of the indelicate obvious · Strategy canvas

Introduction

In broad terms, a **threat** is a menace, which is a source of danger that presents the potential for causing harm. It follows, then, that a severe threat poses existential danger. In the context of a threatened entity, person, or institution, such a threat can take many forms, most of which broadly divide between natural disasters and induced catastrophes (Antokol and Nudell 1988, p. 3).

A threat capable of being anticipated, however, is a threat that can be mitigated or managed. Thus, even in the face of devastating natural disasters, planners, political leaders, and responders generally have an idea of what to expect. Areas susceptible to hurricanes tend to have more resources for contending with evacuation than with avalanche, just as areas prone to earthquakes tend to pay more attention to building codes that impose requirements for seismic hardening. Similarly, when it comes to induced catastrophes, such as a frontal attack by an opposing army, nations threatened know where to array their defenses, where to add fortification, and how to equip a counter force with air, sea, and ground assets that will either deter an adversary or exact a high price for any attack.

When it comes to insider threats, however, the defender's focus necessarily shifts. Traditional defenses no longer serve so readily to defeat attackers or mitigate foreseeable dangers. Why? An insider threat is by definition a menace that operates within the protected area of established defenses. More specifically, for the purpose of the discussion that follows, **an insider threat is defined as 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 institution being targeted**. Hostile or malicious insider and trust betrayer may also refer to whoever represents an insider threat, although these two terms focus more attention on the individual than on the phenomenon (Catrantzos 2012, p. 4).

Scope

For the purpose of this chapter, **insider threats are** the kind of **serious menaces which are induced**, namely, the work of adversaries operating against the individual or entity being attacked, **as opposed to** natural disasters, accidents, or adverse events **arising out of chance**. Consequently, this focus on insider threats includes in its province discussion of infiltrators, trust betrayers, and maleficent actors bent on causing harm to people or organizations. Individuals and actions that cause harm as the result of mismanagement, ineptitude, or inattention, however, are beyond the scope of the operating definition of insider threat, hence excluded from discussion here.

Status Quo

As of early 2018, many disciplines have contributed to insider threat studies, including the burgeoning fields of workplace violence, treason and espionage assessments, and psychological and social motivation research. However, the one discipline presently dominating the insider threat arena is cybersecurity, as typical reporting on insider threat concerns and investments reveals a near exclusive focus on "trusted access to computer systems and data (Benoit 2017)."

Indeed, the cyber-centric view of the insider threat challenge can take on an incestuous character. This becomes evident when white papers predictably advise more cyber controls, are sponsored by information technology vendors, and are written by career technologists who infuse such studies with much opinion overlaid on the kind of survey data expected of a cyber-focused clearinghouse that publishes such reports (Cole 2017).

While the cyber-centric focus offers value, its attending concentration can limit attention to the broader threat picture that is not exclusive to the use of technology to counter insider attacks as well as on technology's vulnerability to penetration and hostile manipulation to cause the same kind of existential damage from a safe remove that an informed operator would otherwise be able to visit only from within the most defended areas.

All insider threat-related disciplines come with their long-term adherents and specialists, along with supporting funding streams that enable concentrating on one particular attack vector at the exclusion of others. This work examines insider threats through the broader lens, however.

The cyber-centric approach sees insider threats and defenses largely as a matter of electronic access, credentials, safeguards, online monitoring, and, more recently, the infusion of artificial intelligence and predictive analytics for spotting hostile insiders operating within the secure perimeter of a given institution (Evanina 2017). To the extent that this approach delivers innovations that include automated detection of untoward activity by trust betrayers in order to enable identifying them after an insider attack, the approach offers some value in after-the-fact event reconstruction and prosecution of attackers. To the extent that it enables blocking or actively thwarting attacks before there has been serious harm, the value increases many fold. However, to the extent that cyber-centric defenses introduce burdens into the workplace that grow to be out of proportion to the value sought, these approaches raise questions and inspire critics even from their own ranks (Herley 2009; Donovan 2016).

Unifying Thread of Conventional Defenses

The one unifying thread that runs through most conventional approaches to defending against insider threats, whether focused on cybersecurity, counterespionage, or workplace violence prevention, is a canonical reliance on experts and a general exhortation to all lay individuals to refer insider threat concerns to these experts for guidance and resolution. Direct exposure to any reasonable incidence of threats from hostile insiders soon uncovers the built-in self-sabotage of this advice.

Advising the lay co-worker and manager to leave a given matter to the experts (sometimes abbreviated as LITE, for leave it to the experts) only avails if (a) genuine experts exist and (b) those experts are in abundant supply on short notice in order to service the demand for their expertise. Quotidian experience in any work force often raises doubts about the former (a), while also suggesting that the latter (b) is an illusion.

Modern workplace realities suggest that there is wide variation in what passes for an expert on insider threats. If the kind of threat at issue touches on workplace violence, the expertise, so-called and often self-styled, will likely come in the form of a psychologist trained and experienced in assessing the danger posed by the individual showing signs of inflicting harm; of a labor attorney who has previously dealt with such cases; of a security manager who is familiar with how to protect potential targets and how to discreetly monitor the individual suspected of being most likely to cause harm; and of an employee relations representative who must at once balance the rights of the allegedly threatening employee with those of other employees who feel endangered. Add an online component such as threatening e-mail or social media postings, or potential use of computers to cause harm via

remotely controlled attack, and one or more cyber professionals join the ranks of experts to be consulted.

In most organizations, insider threats remain statistically rare (Shaw and Fischer 2005). However, if by chance there were to be more than two cases surfacing at the same time, the attending burden would rapidly overmatch the availability of experts on hand to address those cases. Consequently, any institution that intentionally excludes the larger work force from an active role in addressing insider threats necessarily sets itself up for uneven or unsatisfactory performance.

There will seldom be enough experts to meet the demand, particularly if multiple cases arise at once. Moreover, the more complex the case, the more experts the organization will summon to address it, thereby increasing the chances of delay in convening all the experts because of inevitable scheduling conflicts. Meanwhile threats remain in place, variously simmering or even coming to a boil before all the "experts" can bring their unique insights to bear on the problem.

Attempting to compensate for this imbalance between demand for and availability of experts may lead the institution to impose more Procrustean controls and invasive monitoring, on the theory that such measures will aid in the early detection of insider threats. However, this approach alienates the lay employee population all the more, as it is the latter who must shoulder the additional burdens to transacting normal business for a benefit that few will ever see or actively associate with their own protection. Such is the case, for example, with burdensome imposition of requirements to regularly change passwords which a Microsoft engineer dubbed externalities in his analytical study of how the extra work mandated under the banner of increasing protection turns out to be not only significant but out of all proportion to the benefit sought (Herley).

The tug-of-war that this situation fosters between designated experts and the lay work force they claim to defend from insider threats accounts for why many insider threat programs fall short of their advertised promise, and this emerges in the next section as a closer examination of the nature of insider threat defenses begins to take shape.

Limitations of Conventional Wisdom

Accepted wisdom has highlighted the predominance of the disgruntled insider as the kind of hostile trust betrayer meriting closest scrutiny, while also offering up default solutions in the form of invasive monitoring and tighter controls overseen by experts. However, an alternative analysis that began where these approaches end ultimately arrived at research-based conclusions that pointed to the flaws in these approaches and suggested an alternative approach, viz., No Dark Corners (Catrantzos 2009, 2010a).

Type of Insider: Disgruntled Employee vs. Infiltrator

The first flaw is in assuming a greater level of threat posed by a disgruntled employee as opposed to an infiltrator. While conventional wisdom suggests that the disgruntled insider will already possess a higher level of access and intimate knowledge of the inner workings of an institution that better equip him or her to carry out a devastating attack, workplace reality tells a different story about how much of an existential threat such a hostile insider poses.

Troubled employees signal their discontent, eventually alienating those around them, at least to the point of disqualifying themselves from positions of greater trust and responsibility. As malcontents, they often become harder to manage, which also makes them a potential liability if being recruited by an adversary, such as a terrorist cell, for a role in carrying out an act of sabotage or mayhem. Moreover, as a behaviorist participating in a research study suggested, based on extensive experience in dealing with threatening employees and the aftermath of workplace violence, the disgruntled insider tends to be seeking not so much victory as relief from a situation perceived as unbearable (Catrantzos 2012, p. 323).

An infiltrator, by contrast, is more amenable to training, preparation, and insertion into a targeted institution. Such an individual has already been recruited, disciplined, and motivated by a belief in his cause. In terms of potential usefulness to a terrorist cell, a well-placed infiltrator is a guided missile, while a disgruntled employee is more likely to be a loose cannon. Where conventional wisdom assumes the infiltrator will be thwarted is in the vetting process that relies on a background investigation and other organizational mechanisms which the institution is assumed to be able to deploy adroitly to screen out insider threats. Closer examination of workplace realities, once again, reveals the folly of such assumptions.

Achilles' Heels in Countering Insider Threats

(a) Reliance on Background Investigations
Background investigations do not by themselves weed out inept, unreliable, or dangerous employees, including maleficent applicants seeking employment with the goal of causing harm. Why? A background investigation is a snapshot in time, usually of limited scope, that gives a certain view of an individual that may or may not inform an employment decision. Much depends on who is reviewing the background investigation report and how the institution is using that information as part of a comprehensive vetting process. Moreover, the way in which a new hire is monitored and carefully assessed for retention at the conclusion of a probation period does more to weed out bad and potentially dangerous employees than reliance on any background investigation alone (Catrantzos 2012, pp. 75–91).

(b) Reliance on Specialists or Corporate Sentinels

A manifestation of the widespread institutional predilection to leave this problem to the experts (or LITE), this tendency marginalizes co-workers and front-line supervisors to the point of making them only passive reporters of suspicions, thereby denying them a positive role in thwarting insider threats before the latter have had a chance to cause a major loss event.

(c) Tightening Controls as Default Means of Defense
When in doubt or when suspecting an insider threat may be imminent, organizations typically respond by increasing invasive measures and adding burdens for all employees. This has the effect of punishing the blameless for the assumed transgressions of unseen adversaries. On a basic level, for example, if the employer's prime insider threat concern is that of penetration of the network, then knee-jerk countermeasures typically begin with imposing more complicated and more frequent password changes on the part of the entire employee population. Not only do such measures inspire employees to circumvent burdens by recording their passwords where they may be exposed to compromise, they also can become so counterproductive as to encourage the rule-givers themselves to ignore such impositions (Herley, Donovan, op cit).

Self-Defeating Aspects of Default Responses

The foregoing defenses underscore the self-defeating nature of these approaches in which the common thread that unravels the defenses is a lack of active involvement on the part of the work force on the one hand, tied with what workers perceive as the offensiveness of too much oversight on the other hand. Moreover, an overbearing vigilance against disloyalty, according to one student of trust betrayers, "threatens the ecology of trust and raises the likelihood of disloyalty because of a motivation to resist excessive oversight (Carney 1994, p. 21)." Marginalized and overburdened employees soon make it their goal to bypass oppressive controls.

At the same time, the institution tells the work force that insider threats are the exclusive province of experts, namely, the usual corporate sentinels of security, human resources, legal, information technology, and human resources departments, as occasionally augmented by psychologists or other specialists. In effect, this LITE approach locks all nonspecialists into apathy, while the specialists often find themselves overextended beyond their resources.

It is in the milieu resulting from these circumstances that wily infiltrators can maneuver themselves into a dark corner from which to perform pre-strike reconnaissance and target selection before carrying out insider attacks with relative impunity and a good chance of inflicting severe damage before being caught or deterred.

No Dark Corners as Insider Threat Defense

The Dilemma: A Problem with the "Problem"

The insider threat challenge is complex, multifaceted, and resistant to reflexive or Procrustean remedies. As such, it takes on the characteristics not so much of a problem but of a predicament, hence its immunity to the measures conventional wisdom advocates. Most people, according to one observer of this kind of dilemma, see themselves as problem-solvers, which limits their capacity to recognize and contend with predicaments (Farson 1996, pp. 6–7).

Problems succumb to straightforward solutions. When those solutions fail to produce immediate results, the problem-solver tends to increase the dosage rather than alter the treatment.

Predicaments, on the other hand, defy linear, traditional thinking. Instead, they require interpretive thinking and the capacity to put a larger frame around the situation in order to grasp it in its multiple contexts. Such is the case with the insider threat.

Toward a Solution

If the insider threat is indeed more predicament than problem, it stands to reason that a mere accumulation and doubling down of reflexive countermeasures will disappoint or provide uneven results. Consequently, the interpretive thinking required for addressing predicaments must come into play. This, in turn, requires leaders responsible for bringing the situation under control to display a higher order of decision-making. One chronic student of organizations who began as an economist making financial projections for large institutions before launching multiple ventures of his own and ultimately attaining affluence and a cachet in unrelated fields characterized this kind of intelligence on a three-level scale (Adams 2018) (Fig. 1).

The lowest level of the scale represents the lowest form of intelligence, namely, that which operates with few if any facts. Individuals operating at this level follow precedent or echo whatever platitude is most convincingly vouchsafed them. In the context of an insider threat, employees functioning at this level would detect or thwart a hostile insider only by chance.

The next level is the province of individuals who have accumulated many facts or specialized knowledge. Confident that they know more about a given problem than those on the lowest level who lack such detail, they employ their knowledge in a way they perceive to be superior not only to the ones below but often to those above them in the institutional hierarchy. This is the province of the experts, of the sentinels who think that because they have mastered some arcane aspect of insider threat studies, they and only they are qualified to address whatever threat may be at hand.

The highest level of intelligence, however, consists not of knowing as many facts about the problem as possible but of knowing which facts matter. In the case of insider threats, this level would be the province of decision-makers who have to

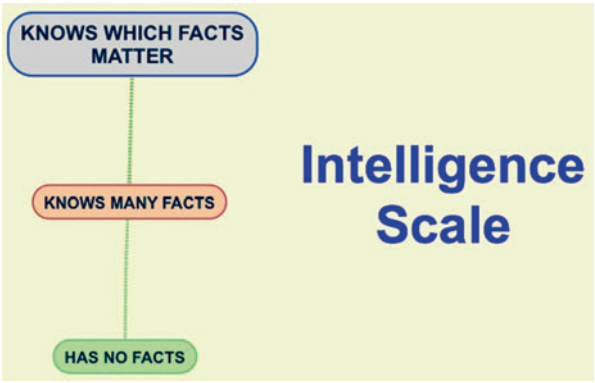

Fig. 1 Intelligence scale

select a course of action or set a policy. At this level, performing effectively requires the ability to make a timely decision, rather than waiting for more facts to arrive in order to point to the right decision. This waiting loses the moment to act in time to avert catastrophic loss. Being able to seize this moment, however, requires making peace with more uncertainty and gaps in detail than many risk-averse experts are capable of tolerating.

To those capable of functioning at this third level, a different approach which engages instead of alienating the work force offers more promise than traditional overreliance on draconian measures and condescending sentinels. Moreover, such decision-makers also realize that the prime goal of insider threat defense should be preventing loss rather than building an ironclad case for prosecuting whoever was responsible for causing it.

Enter the No Dark Corners Approach

This approach to tackling the insider threat from a different perspective traces to a Delphi research study that was the subject of an award-winning thesis at the Naval Postgraduate School and which appears in condensed form in a peer-reviewed professional journal (Catrantzos 2010a). The essence of this approach includes (a) overhauling the background screening or vetting process, (b) placing monitoring and screening responsibility at the co-worker level rather than in the exclusive hands of distant experts, and (c) broadly fostering an environment where co-workers function not as informants but as copilots who are taking an active hand in their own protection. The ultimate aim of this approach is opportunity denial. In other words, deny hostile insider opportunities for causing harm by eliminating their ability to exploit the institutional vulnerabilities that current defenses allow to linger in place, namely, the dark corners which an adversary needs to be able to penetrate and strike from in order to inflict maximal damage.

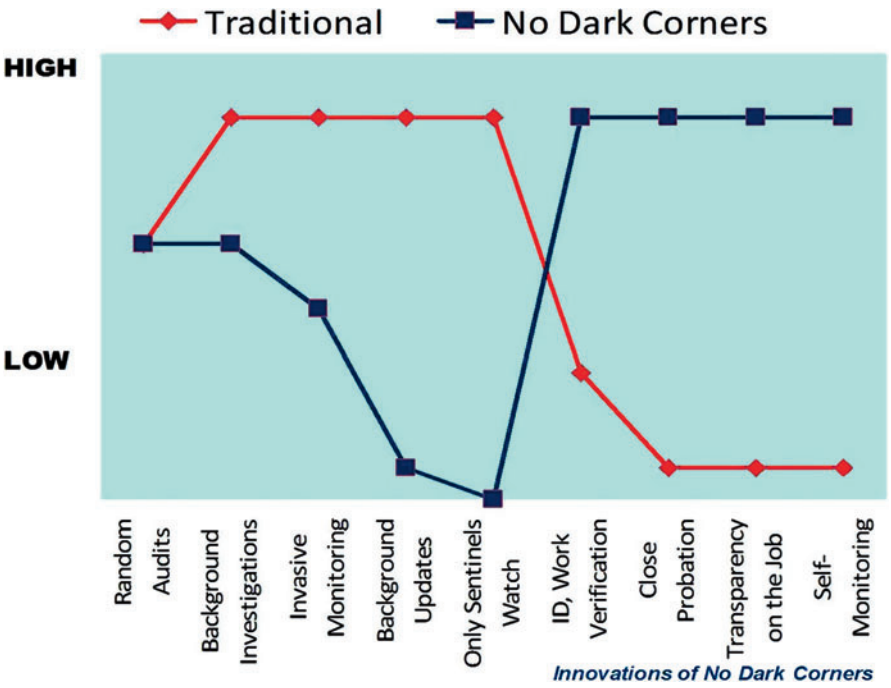

Fig. 2 No Dark Corners Strategy Canvas

Differences in Context

The strategy canvas that follows represents traditional insider threat defenses contrasted against the No Dark Corners approach, using a tool that the creators subsequently made available free of charge via an iPhone application, Blue Ocean Leadership Canvas (Kim and Mauborgne 2005) (Fig. 2).

Point by Point

Random Audits

The reason random audits do little to prevent insider attacks is they are seldom truly random. Their occurrence tends to be predictable, and available resources dictate that they be performed selectively, thus giving a clever trust betrayer ample opportunity to bypass them. Consequently, whereas the traditional approach may place more value on random audits, the No Dark Corners (NDC) approach also uses them but without over-relying on them.

Background Investigations

As noted above, background investigations do not screen out insider threats. At best, it is the intelligent use of the product of such investigations as part of a thoughtful vetting process that does the job. For this reason, NDC, again, avoids ascribing utopian value to background investigations, per se, while increasing their value by paying extra attention to other areas that tradition downplays, namely, identity verification, close probation, and greater engagement at the work team level by emphasizing transparency and engagement of self-monitoring teams (about which more follows, below). Another misapplication of background investigations that the traditional approach occasionally champions is in recommending such investigations for non-employees who have reason to gain recurring access to a given employer's premises and assets. There are other, better ways to handle the related insider threat potential, namely, through the kind of knowledgeable escort that goes hand in hand with more transparency on the job.

Invasive Monitoring

As with other countermeasures, NDC recognizes that invasive monitoring can, at times, alienate more than assist in uncovering hostile insiders. Such monitoring takes the form of imposing draconian burdens on the work force, beginning with annoyances as simple as mandating frequent and complicated password changes for access to networks and applications and ending with what employees perceive as organized snooping to catch them at some policy infraction. Such monitoring leads to counterproductive results, with employees finding creative ways to bypass the monitoring, which opens them to unwittingly making common cause with insider threats in the process (Catrantzos 2012, p. 23). Instead, the NDC approach is to put more reliance on self-monitoring at the team level.

Background Updates

The same organizations that invest their preemployment background investigation with near mythical value tend to either refrain from periodic updates of the background investigation except in circumstances required by law or by policy. Then most update investigations become a mere formality, making their value questionable. By contrast, an NDC approach pays more attention to background update investigations, if the institution conducts them at all, because people change over time. The ingenuous new hire who came through the door smiling as a young adult may not necessarily remain a model employee and valued contributor after experiencing career disappointment and unpredictable life events over the course of many years.

Only Sentinels Watch

The conventional, LITE approach assigns responsibility for threat monitoring exclusively to specialized sentinels like security staff, network administrators, auditors, and labor relations representatives. By overemphasizing this reliance on expert sentinels, the employer in effect marginalizes the value of co-workers who interact

most directly with a potential insider threat and who should ideally be serving as the first line of defense. NDC, by contrast, recognizes that sentinels retain their value but not at the expense of relieving all other employees from taking a hand in their own protection.

Identity and Work Verification

A truism in management and security circles remains that one of the best ways to prevent losses caused by problem employees is to avoid hiring problems in the first place. One of the oft-neglected means of assuring that future problem employees be screened from the applicant pool is the careful verification of their identity and other qualifications for employment. Given the widespread rise of identity theft and relative ease of falsifying credentials, NDC takes a closer look at such verifications, while traditional recruiting functions operate under a greater incentive to speed applicants through a hiring process because they rely on the background investigation as their sole failsafe.

Close Probation

Under conventional circumstances, the typical probation process is a mere formality regulated by the passage of a prescribed period of time. In other words, if the probation period is 6 months and the new hire has committed no egregious transgressions within that half year, passing probation is a given. The NDC approach, however, turns the tables completely, giving the probation process much greater consequence. Under NDC, the default becomes that a new hire will not pass probation unless he or she demonstrates both ability and compatibility as gauged at the work team level. Consequently, if any member of the work team has misgivings about the probationary new hire, the latter is summarily released at the conclusion of the probation period – if not sooner. This policy reversal makes the team responsible for weeding out poor or suspect performers before they have a chance to become bad employees who would then become much more difficult to terminate once having passed probation.

Transparency on the Job

With NDC's emphasis on transparency on the job, the new default becomes for critical tasks and operations to be performed in actual or virtual line of sight of a peer or team member acting not as a snoop but as a copilot (Catrantzos 2010a, p. 22). Work becomes designed to maximize visibility to peers in order to improve overall performance. This approach also results in minimizing opportunities for clandestine attack or sabotage. Moreover, where the employer lacks the staffing to support implementing this kind of a buddy system, it is here that an infusion of technology shows great promise. It is here that remote collaboration by sharing of video or introduction of artificial intelligence to assist with the detection of anomalies may not only deter malicious acts but also prevent accidents that a lone employee might otherwise cause in the absence of another set of eyes and ears. It is also in this space that knowledgeable escort comes into play as a means of assuring that outsiders who require temporary insider access do not abuse that access to carry out attacks.

(Expanded discussion of knowledgeable escort continues in the section which follows.)

Self-Monitoring at the Team Level

Audits most effectively deter insider threats when carried out at the work team level by team members themselves (Catrantzos 2010a, p. 23). Thus, team members shift the focus from the traditionally adversarial audit approach of catching employees doing something wrong to an NDC value-added approach of finding ways to do things better. This change of focus necessarily complicates the effort of an infiltrator or hostile insider who may be adept at eluding corporate sentinels and traditional audits but finds nowhere to hide among an alert team that is fully engaged in exercising a proprietary interest in the job.

Prominent Aspects of Insider Threats and Promising Defenses

Insider threats retain certain signature features, as do some defenses against them. Both threat and countermeasure, however, also show weaknesses as well as capacity for adaptation. Some of the signature aspects and promising defenses against them include the following:

Deception

A frontal attack makes few demands for subtlety on the attacker's part. Force meets force, and victory goes to superior might, arms, and strategy. With insider threats, however, no attack can be successful without some measure of deception. After all, the mere gaining of insider access requires being able to gain trust, pass scrutiny, and maneuver into a position from which to inflict harm. None of this is possible without the ability to deceive, i.e., to earn the trust that one intends to betray. For this reason, deception remains the insider threat's stock in trade.

Consequently, it stands to reason that defenders should be adept at detecting deception. However, research evaluating competence over a period of decades suggests that defenders barely perform above the level of chance (Colwell et al. 2006).

Defenders may find it useful to study one or more methodologies used in the workplace to detect deception, including scientific content analysis, the Reid Technique, the Wicklander-Zulawski method, behavioral detection, or old school, legal cross-examination (Catrantzos 2012, pp. 95–107). All of these tools have adherents and critics, yet none is foolproof or easy to apply without significant investment in time, training, and practice.

One alternative is the NDC approach to uncovering deception by hostile insiders by focusing on anomalies and calling upon multidisciplinary assessment teams of the kind used with some success in countering threats of violence at schools (Catrantzos 2012, p. 118). Pioneers exploring this technique leveraged the mature

research arm of the US Secret Service that studied the behavior of would-be presidential assassins and later made common cause with the US Department of Education in the wake of the 1999 Columbine school shooting, ultimately arriving at this three-step approach (Fein et al. 2002):

(a) Use multidisciplinary teams, instead of relying on a single expert, particularly when institutions may not have ready access to on-site experts.
(b) Give priority attention to whether the insider under scrutiny actually poses a threat more than on whether he or she articulated a threat.
(c) Accord prompt attention to every threat.

Knowledgeable Escort

The real issue in countering insider threats is not so much the status of the hostile insider as employee, vendor, or contractor but access to critical operations and assets. While it is impractical to perform background investigations on every person who ever requires access to a critical area, it is equally foolish to assign an escort who does not possess the technical expertise necessary to tell whether the outsider being monitored is performing a required task or doing something more maleficent (Catrantzos 2012, p. 87). Escorts must be able to distinguish sanctioned from unsanctioned activity and also able to intervene in time to prevent or at least limit damage. Thus, neither a secretary nor a surgeon should be conscripted to escort a technician working on the employer's network, any more than a corporate attorney should be asked to act as escort overseeing the work of an alarm technician. Each case requires a knowledgeable escort, or an overseer who possesses the right skills to ensure that the work under review is being done properly.

The realm of knowledgeable escorts is one which shows promise for the harnessing of artificial intelligence to supplement shortages of available specialists on staff to perform this kind of monitoring. This may prove a better application of research currently being examined for using artificial intelligence as a means of predictive analysis for spotting which insiders may be prone to posing a threat (Evanina, op cit).

Additionally, experimental robots making their debut at electronic industry trade shows include a model that can work with customers at a supermarket, answering questions of price, and even guiding them through the aisles (Choudhury 2018). Such an advance could show promise for the knowledgeable escort of the future.

Curse of the Indelicate Obvious

The curse of the indelicate obvious is an institutional dilemma befalling organizations when a disproportionate fear of defamation suits, accusations of discrimination, or obsession with political correctness leads the people in charge to ignore glaring indicators that something could be seriously wrong (Catrantzos 2010b). Thus, an

employee with gang tattoos or a new car worth more than his annual salary eludes closer examination when common sense would suggest that such an individual may bear more scrutiny or at least merit involvement in some fact-finding interview as opposed to being ignored or held on a par with other, more closely vetted employees. From a view of insider threat defense, obvious warning signs are not smoking guns establishing guilt in and of themselves. However, they do deserve a second look, no matter how indelicate or awkward it may be to suggest taking that look.

Lawful Disruption

Lawful disruption, in the context of insider threat defense, is the thwarting of attack through legally permissible means (Catrantzos 2012, pp. 135–136). One of the chief distinctions of lawful disruption from traditional law enforcement action is that the former accords top priority to prevention, while the latter tends to give precedence to prosecution. Indeed, actions that deter potential attackers to the point of leading them to select other targets do little to make a legal case against those would-be attackers. At the same time, defenders can find in lawful disruption a much higher value than in the combined investment in staffing and technology it may take to reconstruct who was responsible for an attack only after that attack has taken place. Thus, lawful disruption offers the lay defender a means of making a positive contribution before witnessing losses of life and critical assets.

Lawful disruption flows seamlessly into an NDC approach where employees exercise a proprietary interest in their job and the assets under their stewardship. Such employees need little urging to approach any individuals seeming out of place. Their genuine curiosity and concern legitimize offers to help these individuals to find their way. At the same time, however, such personal contact communicates to adversaries that this site is staffed by watchful employees, hence a harder target than those workplaces where no one pays attention to people who do not belong there.

Copilot Engagement vs. Draconian Alienation

Behavioral economics reveals that events which destroy trust are more noticeable and carry more weight than events that build trust (Just 2014). Thus, invasive monitoring and draconian controls that burden employees under the banner of defending against insider threats serve more to alienate the very employees from whom management seeks voluntary compliance.

By contrast, the NDC model aims to transform every employee not into an inquisitor but a copilot who has a vested interest in the shared objectives of other team members (Catrantzos 2009, p. 54). In the genuine sense of copilot, every team member becomes the equivalent of a qualified pilot who assists or relieves the pilot but is not in command. In this context, copilot engagement produces cohesion rather than alienation because it demonstrates a shared sense of ownership in the team's

work. Consequently, electronic extensions of the copilot model become a welcome means of summoning assistance instead of a manifestation that management does not trust the employees and must therefore keep them under remote surveillance.

Defensive Strategies at the Societal Level

As some observers of societal trends have remarked, changing demographics affect culture because the fastest-growing population group dictates culture (Drucker 2002), and the emerging dynamic of tribalism increasingly appears to take precedence over loyalty to the larger commonwealth (Hanson 2017). Under these circumstances, there is a case to be made for looking at large, disaffected groups within a nation as potentially forming societally malicious insiders that threaten to tear the fabric of the culture that has heretofore underpinned the nation that played host to such groups when the focus of their grievances was elsewhere. Within this larger frame, some research findings on insider threats may apply to the broader challenge of understanding and countering this type of societal insider threat.

Significance of Divided Loyalties

One seldom advertised epiphany that was the product of decades of studies in treason unearthed a noteworthy change over time in the makeup of modern-day traitors. Specifically, the researcher conducting these studies discovered that today's traitors are much more likely to be motivated by divided loyalties than by the kind of financial motives that prevailed as recently as the 1980s (Herbig 2008).

Some illuminating perspective begins to surface in taking this thought of divided loyalties in juxtaposition against other forces rending the traditional social fabric that used to wrap fellow citizens in a certain common garb that reinforced shared identity. For example, it is plausible to infer that in present Western society, there arises a divided loyalty between what one may think of as loyalty to one's country and X, where X is a social identity that may be along the lines of race, religion, or even more so for an ideology that elevates, say, Sharia supremacism over a law of the land such as the US Constitution or Napoleonic Code. Extending this hypothesis, one may argue that, with the erosion of traditional civics and history education that instills pride of country, the X loyalty is almost certain to take precedence over the national loyalty.

What does this mean? Alas for national security and what may have once been defined as old school patriotism. A young adult steeped in this new world will find a natural tendency to gravitate to X and, in so doing, do this at the expense of his or her country, society, and remaining, frayed threads of a culture that the media may portray as oppressive, irrelevant, or discriminatory.

Defensive Options

What is the solution? This is a question harder to answer on the societal level than on an institutional or employer level. However, if the principle of cohesion-based engagement can extend from an employer to an entire nation, perhaps a useful starting point may be to aim at reversing the priority of divided loyalties. The objective, then, becomes to start by doing something to elevate loyalty to country over X, whatever X may be. In other words, the objective would be not to urge citizens to shun their loyalty to X, which may define them in many ways, but to just prioritize the country which houses, hosts, and provides them a decent life one step above that particular X.

Some potential cohesion-building options to explore could include mandating some form of national service, requiring fluency in one lingua franca as the official language for the conduct of business in a given nation (without penalizing fluency in multiple languages), and making widespread demands of citizenship that include a basic understanding of the history and founding principles of the host nation.

Early Warning and Preemption

If efforts to increase cohesion lag or falter, there may be other No Dark Corners approaches that avail. For example, one observer sounding the alarm over American susceptibility to terrorist attack on the domestic front advised that citizens take on a new role as first preemptors rather than first responders, because the number of official responders in a position to actively thwart terrorists at home amounts to less than 1% of the US population (Ruffini 2006).

This advice runs in harness with the larger NDC approach of having employees – or, in this application, lay citizens – take an active hand in their own protection. Opportunities for increasing citizen involvement in active defense of this kind can easily include widespread promotion of guidance on how to perform the kind of lawful disruption that can frustrate or deter terrorist attacks without putting average citizens at risk.

Other Options

Other options to explore include:

- Making organized use of returning veterans as emergency volunteers to assist with life-saving activities in the immediate aftermath of a mass casualty terrorist attack at home.
- Giving Good Samaritan protections to trained and vetted citizen volunteers who are willing to physically engage with attackers before they can inflict more casualties without waiting for police to arrive on scene.

- Instituting tort reform to limit frivolous claims for damages which may otherwise prevent citizens from alerting authorities to the kind of suspicious activities that are precursors to a terrorist attack.
- Withdrawal of privileges for assessed and validated threats to society, including revocation of citizenship or exile, provided this can be done with due process.

Concluding Observations

Insider threats are persistent, adaptive, and resilient because the insider threat is more predicament than problem. Accordingly, where traditional approaches fail to yield desired results, it is necessary to adopt more innovative approaches. One such approach, No Dark Corners, or NDC, is about an idea.

The idea is about how to control – at the team level – the work spaces and critical assets that all employees or citizens use and are responsible for on a daily basis.

NDC is about turning what is traditionally cast as the weakest link into the first line of defense, about moving protection from the sidelines to the front lines. It is about reasonable human beings' meaningful engagement in their own protection, including management, the sentinels whose official job it is to look for insider threats, and – most importantly – the people at the work team level, co-workers turned copilots, who are mostly ignored yet remain the most effective at spotting and thwarting insider threats.

Epiphanies

The nature of the threat limits the options for uncovering new insights about it. Statistical studies via quantitative research offer limited yield, in part because insider threats remain statistically rare. Most people, most of the time, do not go around betraying trust or stabbing each other in the back.

However, rare does not mean nonexistent. Betrayal still occurs, and it is all the more unpleasant and devastating when it comes by surprise.

By definition, insider threats are not frontal attacks. Otherwise, they would be outsider threats. Consequently, if the attack is coming from within, a certain degree of surprise is inevitable. This surprise requires deception, and deception can be detected, therefore countered.

Not all insider threats are existential. Indeed, most of them aim short of carrying out attacks fatal to the organization. The trouble is, as a defender, one cannot always tell the difference in advance.

Conventional wisdom sounds good and keeps resurfacing because it aligns well with familiar approaches. As one study noted, "professionals often choose the tools with which they are most familiar: Police officers arrest; mental health professionals commit; workplace managers fire; principals suspend or expel (Fein et al., p. 64)."

Doing more of the same is the default advice, yet results do not necessarily align with intensity. More is not always better. More is not even enough. When it becomes

oppressive, it can become too much, as do invasive monitoring and ever-increasing controls that burden the work force unduly.

An effective defense against insider threats is more likely to result from a multipronged approach like NDC than from overreliance on a single, heroic solution that is more problem-oriented than responsive to a larger predicament. It is akin to how an aikido instructor characterized self-defense without the flourishes and hyperbole often expected of martial arts, viz.,

> Effective self-defense is surviving daily life using all your tools. It is careful driving, eating right, using your body as it was designed to be used. It's soap and water and flu shots. It's doing your homework, paying bills on time, dealing honorably with others. It's batteries in the fire alarm, knowing how to swim, all the bits and pieces that make up daily life. Real life. (Shifflett 1999)

References

Adams S (2018) "Intelligence scale," Theme of second *Periscope* broadcast of Jan 4, 2018. Retrieved 4 Jan 2018 from https://www.pscp.tv/w/bR07HDFEWUVYVnFMcnh2S2d8MXJteFBPQVJ2QmdKTkoDwNfw0-C7hWoOCobaYJXCiC6ZdBbJHTrviP6VbJYX

Antokol N, Nudell M (1988) The handbook for effective emergency and crisis management. Lexington Books, Lexington, p 3

Carney RM (1994) The enemy within. In: Sarbin T, Carney R, Eoyang C (eds) Citizen espionage: studies in trust and betrayal. Praeger, Westport, pp 18–38

Catrantzos N (2009) No dark corners: defending against insider threats to critical infrastructure, MA thesis, Center for Homeland Defense and Security, Naval Postgraduate School, Monterey

Catrantzos N (2010a) No dark corners: a different answer to insider threats. Homeland Secur Aff 6, Article 5. Retrieved 3 Jan 2018 from https://www.hsaj.org/articles/83

Catrantzos N (2010b) Defending against the threat of insider financial crime. *Frontline Security*, pp 17–19. Retrieved 6 Jan 2018 from http://security.frontline.online/content/insider-financial-crime

Catrantzos N (2012) Managing the insider threat: no dark corners. CRC Press, Boca Raton

Choudhury SR (2018) Tech giant is rolling out new robots to replace workers in hotels, airports and supermarkets, *CNBC Business News*, January 4, 2018. Retrieved 4 Jan 2018 from https://www.cnbc.com/2018/01/04/south-koreas-lg-electronics-to-introduce-new-robots-at-ces-2018.html

Cole E (2017) Defending against the wrong enemy: 2017 SANS insider threat survey, *SANS Institute InfoSec Reading Room*, Sponsored by Dtex, Haystax Technology, and Rapid 7, August 2017. Retrieved 18 Aug 2017 from https://www.sans.org/reading-room/whitepapers/analyst/defending-wrong-enemy-2017-insider-threat-survey-37890

Colwell LH, Miller HA, Lyons PM Jr, Miller RS (2006) The training of law enforcement officers in detecting deception: a survey of current practices and suggestions for improving accuracy. *Police Q* 9(3):275–290

Donovan F (2016) IT admins to users: do as I say, not as I do: survey of IT admins at RSA finds some IT admins never change admin credentials at all, *RSA Conference Survey*, April 7, 2016. Retrieved 5 May 2016 from http://www.fierceitsecurity.com/story/it-admins-users-do-i-say-not-i-do/2016-04-07

Drucker P (2002) Managing in the next society. Truman Talley Books St. Martin's Press, New York, p 36

Evanina B (2017) Defusing leakers means knowing what makes them tick, *The Cipher Brief*, September 13, 2017 (issue on tackling insider threat ranging from leaking classified information

to workplace violence, in interview of National Counterintelligence and Security Center Director Bill Evanina). Retrieved 18 Sept 2017 from https://www.thecipherbrief.com/column/strategic-view/defusing-leakers-means-knowing-makes-tick

Farson R (1996) Management of the absurd: paradoxes in leadership. Simon & Schuster, New York, pp 6–7

Fein RA, Vossekuil B, Pollack WS, Borum R, Modzelski W, Reddy M (2002) Threat assessment in schools. U.S. Secret Service/U.S. Department of Education, Washington, DC, pp 33–38

Hanson VD (2017) Nation v. Tribe, *Defining Ideas: A Hoover Institution Journal*, December 6, 2017. Retrieved 8 Jan 2018 from https://www.hoover.org/research/nation-v-tribe

Herbig KL (2008) Changes in espionage by Americans: 1947–2007, *Technical report 08–05*. Defense Personnel Security Research Center, Monterey

Herley C (2009) So long, and no thanks for the externalities: The rational rejection of security advice by users, In: Proceedings of the new security paradigms workshop, Oxford, 8–11 Sept 2009, pp 1–12

Just DR (2014) Introduction to behavioral economics. Wiley, Hoboken, pp 465–466

Kim C, Mauborgne RA (2005) Blue ocean strategies. Harvard Business Press, Boston, pp 12–15

Ruffini JA (2006) When terror comes to main street. Archangel Group, Denver, p 201

Shaw ED, Fischer LF (2005) Ten tales of betrayal: the threat to corporate infrastructures by information technology insiders. Defense Personnel Security Research Center, Monterey, p 34

Shifflett CM (1999) Aikido exercises for teaching and training. Round Earth Publishing, Berkeley, p 20