1-2024

Understanding Insider Threats: Learning from Related Research Streams

Matthew Allen
University of Nebraska at Omaha, matthewallen@unomaha.edu

Kat Parsons
National Counterterrorism Innovation, Technology, and Education, Center, katherineparsons@unomaha.edu

Tin L. Nguyen
University of Nebraska at Omaha, samuelhunter@unomaha.edu

Lauren Zimmerman
University of Nebraska at Omaha, lzimmerman@unomaha.edu

Understanding Insider Threats: Learning from Related Research Streams

This state of science review summarizes practitioner-oriented and behavioral and social science literature related to insider threat. Practitioner perspectives reveal both overlapping and unique risk factors from cases of espionage, sabotage, and workplace violence. Social and behavioral science research points to the value of focusing on dynamic risk factors for engaging in destructive behaviors, as well as potential organizational interventions that could deter and mitigate insider threat risk.

Major Takeaways

Both practitioners and researchers tasked with detecting and mitigating insider threats should look to related sciences for additional lessons to bolster their efforts. Practitioners and researchers should strive to work across disciplines to help overcome the siloing of the insider threat space.

- **Takeaway 1: There is a range of literature to draw from that can deepen our understanding of malicious insider threat risk.**
  - Implication of takeaway 1: Models of insider threat should account for probability differences in risk indicators by types of malicious threat events and insider motives for harm. Resources outside of the traditional insider threat space can deepen practitioner understanding and prevention efforts.
- **Takeaway 2: Broadening our conception of insiders (i.e., acknowledging levels of organization access and "insiderness") can improve our understanding of insider threats.**
  - Implication of takeaway 2: Delineating levels of organization access can help researchers and practitioners distinguish between those who proactively enter organizations to cause harm to the organization (e.g., espionage) versus its members (e.g., violence against spouses at work or employees by customers), and those who develop grievances over time within their tenure in an organization (e.g., slacking at work or destroying pertinent knowledge in response to unfair work policies).
- **Takeaway 3: Examining multiple types of harmful insider behaviors provides a more complete picture of insider threats to organizations.**
  - Implication of takeaway 3: Clearly distinguishing risk factors and warning signs for specific insider threats better informs practitioners to detect potential harm and lays the foundation for effective, comprehensive counter-insider threat programs.
- **Takeaway 4: The social and behavioral science literature points to new potential methods for reducing and mitigating insider threat risk.**
  - Implication of takeaway 4: Models of insider threat, and particularly positive deterrence counter-insider threat approaches, can be further informed by literature in organizational psychology. Interdisciplinary research that incorporates practitioners offers promising avenues for future practice.

Lessons from Espionage Research

Not all insiders are spies, but most spies are insiders.

- Espionage, or "spying," has changed dramatically in recent years. Modern espionage statutes were born out of Cold War-era politics—that is, major state actors pitted against each other. However, modern spying has shifted dramatically since then, especially in an increasingly cyber-connected world.
    - Espionage statutes are subject to the 'pacing problem;'[1] that is, technology typically moves faster than lawmakers can keep up.
- Espionage typically involves covertly transferring secret or protected information to another adversarial entity.
- However, a more recent trend in espionage cases involves whistleblowers such as Edward Snowden who have sought to release information to the public about their government for issues they believe should receive public transparency (referred to as "leakage").[2]
- Economic globalization and increased use of information systems and technology (IS&T) have created new vulnerabilities to organizations' information assets.
    - As organizations expand their operations and networks across multiple countries, more opportunities for foreign interference arise.
    - IS&T has given malicious actors more ways of accessing proprietary information without physically embedding themselves within an organization. And while the advent of IS&T allows for many advantages for potential spies, it can also make their actions more traceable than in previous generations. That is, people––including spies and leakers––often leave "behavioral residue" (e.g., systems accessed, files moved or changed, information deleted) in their use of IS&T that can be traced back to their use of information systems.

> The Pacing Problem:
>
> "Technology changes exponentially, but social, economic, and legal systems change incrementally"
>
> –Larry Downes, 2009; "The Law of Disruption", p. 2

> "A much bigger worry for spies is that the very vulnerabilities which make it easy for them to steal other people's secrets also make it hard for them to hold on to their own."
>
> –Herbig, 2017, p. 158

Types of Espionage

- **Classic Espionage** is defined as activities done for national government "A," which acts through an agent who clandestinely collects secrets from national government "B" who wants to control those secrets, and who turns them over to national government "A."[3] Classic espionage usually involves theft and requires an alternate identity, false flags, or other deceit.
    - **Economic Espionage,** a type of classic espionage, is the theft of information by or for a foreign government that is a significant enough loss that it could have implications for the entire nation's economy.
- **Leakers** disclose classified information to the public. This is usually accomplished by sharing information through the press or by publication in print or electronic media. A leak often follows the

[1] First described in Downes, Larry. 2009. The Laws of Disruption: Harnessing the New Forces That Govern Life and Business in the Digital Age / Larry Downes. New York: Basic Books.
[2] "Insider Threat Awareness INT101.16." n.d. https://www.cdse.edu/Training/eLearning/INT101-signup/.
Herbig, Katherine L. 2017. "The Expanding Spectrum of Espionage by Americans, 1947-2015." Defense Personnel and Security Research Center Seaside United States. https://apps.dtic.mil/sti/citations/AD1040851.
[3] Herbig, "Expanding Spectrum of Espionage," 64.

form of classic espionage except that the recipient is a public audience rather than an adversarial actor.

Motivations for Classic Espionage

- No single profile for spies or leakers
- In addition, the nature of offenders changes over time, alongside trends in types of espionage
- However, cohort studies dating back to 1947 teach us some lessons about what makes a "spy."
    - Although financial gains often serve as a major motivating factor, those convicted of espionage are almost exclusively middle class.[4]
    - Spies also often have personality features that may distinguish them from their non-spy peers, such as thrill-seeking, narcissistic tendencies, and desire for power and control.[5]
    - There is usually the presence of some sort of critical triggering event that causes acute personal distress.[6] This can include a sudden moral qualm, a personal grievance at the workplace, disgruntlement, economic hardship, or personal problems at home.
    - Personality traits associated with espionage include narcissism, psychopathy, and immaturity, while those associated with mass leaking often include a degree of grandiosity, coupled with personal convictions or a strong moral impetus to serve the "greater good."[7]
    - For classic espionage, the individual must then **not only have access to protected information** but **also a source willing to receive and reward that information**. In the past, this typically referred to a foreign agent responsible for grooming and handling the spy.

> "...recent persons convicted of espionage-related offenses have been male, middle-aged, well-educated, and of a variety of racial and ethnic backgrounds that mirrors the increasing level of education and diversity of American society."
>
> –Herbig, 2017, p. 12

Case Study: Jonathan Pollard

- Jonathan Pollard was a U.S. Navy spy who sold state secrets to Israel. Despite receiving financial gains in return for secrets, he contends that his only motivation was to provide

[4] Thompson, Terence J. 2014. "Toward an Updated Understanding of Espionage Motivation." International Journal of Intelligence and CounterIntelligence 27 (1): 58–72. https://doi.org/10.1080/08850607.2014.842805.
[5] Thompson, "Toward an Updated Understanding of Espionage Motivation"
Wilder, Dr. Ursula M. 2017. "The Psychology of Espionage" 61 (2).
[6] Shaw, Eric, and Laura Sellers. 2015. "Application of the Critical-Path Method to Evaluate Insider Risks." Studies in Intelligence 59 (2): 1–8.
Wilder, Psychology of Espionage."
[7] Herbig, Expanding Spectrum of Espionage."; Thompson, "Toward an Updated Understanding of Espionage Motivation."
Thompson, Terence J. 2018. "A Psycho-Social Motivational Theory of Mass Leaking." International Journal of Intelligence and Counterintelligence 31 (1): 116–25. https://doi.org/10.1080/08850607.2017.1374800.

information to Israel. Further, he claims information sharing should have been occurring already, therefore he was "righting" an existing "wrong."
    - While ideological motivations were likely a component of his espionage activities, the reality is that Pollard also received financial benefits in exchange for secrets, so ideology is unlikely to stand alone as a motivator.

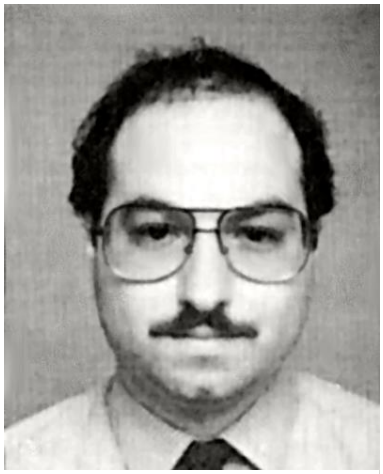


Figure 1—Jonathan Pollard, U.S. Navy I.D. picture. Scanned from Territory of Lies, Wolf Blitzer.

Motivations for Mass Leaking

- Mass leaking is often referred to as "new" espionage, as the digital era allows people to widely disseminate protected knowledge.
- **Unlike classic espionage, a third party is not necessarily involved in either requesting or disseminating protected information from mass leaks**.
- What remains less clear about mass leaking events is whether those engaging in mass leaking share distinct characteristics from those who fit the classic espionage profile. Some previous work has noted that past leakers have shown similar disgruntlement and narcissism as spies, having:
    - strongly objected to something they saw being done in the course of their work (i.e., a moral conviction to act),
    - enjoyed playing the role of expert as holders of "inside knowledge," and/or
    - wanted to help and justified themselves as helping.

- **However, mass leakers are also motivated by a grandiose need for recognition.** These motivations, combined with a media infrastructure that encourages a culture of "non-restraint," help create the conditions for mass leaking.[8]
- Some leakers (as well as spies) are motivated by wealth or other dramatic returns in exchange for their insider knowledge. Others claim purely altruistic or ideological purposes.
    - These motives are not mutually exclusive––that is, if a disgruntled insider already has a desire to serve (a) the public or (b) an adversarial party, but receives further financial or status incentives, mass leakage may become even more likely.
- After the Cold War, the dynamic began to shift to a threat of multiple state actors of ranging power, as opposed to one major superpower.
- Actors working outside of the behest of a nation began to emerge. The increased reliance on IS&T has contributed to this shift by **enabling outsiders access** without needing to **physically infiltrate a facility**, such as in the case of cyberhackers who leak.

Lessons from Sabotage Research

- Whereas espionage entails gathering useful information to further the interests of parties *outside* the organization, the primary goal of sabotage is to interfere with and harm the processes and behaviors of those *inside* the organization.[9]

[8] Thompson, "Psycho-Social Motivational Theory of Mass Leaking."
[9] Giacalone, Robert A., and Paul Rosenfeld. 1987. "Reasons for Employee Sabotage in the Workplace." Journal of Business and Psychology 1 (4): 367–78. https://doi.org/10.1007/BF01018145.

- Sabotage involves intentionally impeding an organization's valued goals by withholding, tampering with, or destroying critical resources (e.g., information, tools, labor) that organization members rely on for their work.[10]

Four Main Types of Sabotage

- **Production:** Production sabotage refers to the deliberate slowing or halting of an organization's production processes.[11]
- **Service Sabotage**: Service sabotage involves behaviors of employees that are intended to undermine customer service and interests.[12] This form of sabotage can occur in any customer-facing role in the service and hospitality industries. Examples of service sabotage include verbal hostility toward customers, delaying service, tampering with customer product orders, and deliberately failing to meet customer service requests.[13]
- **Knowledge Sabotage**: Knowledge sabotage occurs when employees hide key work-related information or share false (i.e., misrepresented or fabricated) knowledge to mislead fellow workers and impede their ability to execute work tasks.[14] Much like service sabotage, knowledge sabotage occurs through interpersonal exchanges, but these behaviors differ in that knowledge sabotage targets co-workers more so than customers.
- **IT Sabotage:** IT sabotage is broadly defined as an insider's malicious abuse of privileged IT system access to cause harm to an organization and its members.[15] This can entail altering, hiding, or deleting important files (manually, or via the installation of bugs and other rogue devices); fabricating information that mocks or damages the reputation of an organization; or disabling employees' access to electronic information, networks, or systems that are vital to conducting their work.[16]

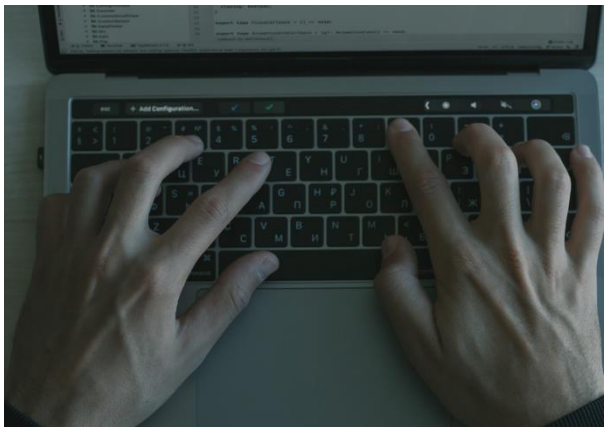
Motivations for Sabotage

- Motivations for sabotage typically stem from self-interest and/or animosity toward an organization and its people.[17] More specifically, people enact sabotage behaviors when they

---

[10] Analoui, Farhad. 1995. "Workplace Sabotage: Its Styles, Motives and Management." The Journal of Management Development 14 (7): 48–65. https://doi.org/10.1108/02621719510097361.
Crino, Michael D. "Employee Sabotage: A Random Or Preventable Phenomenon?" Journal of Managerial Issues 6, no. 3 (1994): 311–30. http://www.jstor.org/stable/40604030.
[11]HOLLINGER, R., & CLARK, J. (1982). Employee Deviance: A Response to the Perceived Quality of the Work Experience. Work and Occupations, 9(1), 97-114. https://doi.org/10.1177/0730888482009001006
[12] Cheng, Bao, Gongxing Guo, Jian Tian, and Ahmed Shaalan. 2020. "Customer Incivility and Service Sabotage in the Hotel Industry." International Journal of Contemporary Hospitality Management 32 (5): 1737–54. https://doi.org/10.1108/IJCHM-06-2019-0545.
[13] Harris, Lloyd C., and Emmanuel Ogbonna. 2006. "Service Sabotage: A Study of Antecedents and Consequences." Journal of the Academy of Marketing Science 34 (4): 543–58. https://doi.org/10.1177/0092070306287324.
[14]Serenko, Alexander. 2020. "Knowledge Sabotage as an Extreme Form of Counterproductive Knowledge Behavior: The Perspective of the Target." Journal of Knowledge Management 24 (4): 737–73. https://doi.org/10.1108/JKM-06-2019-0337.
[15]Band, Stephen R., Dawn M. Cappelli, Lynn F. Fischer, Andrew P. Moore, Eric D. Shaw, and Randall F. Trzeciak. "Comparing insider IT sabotage and espionage: A model-based analysis." CMU-CERT Program, Tech. Rep (2006).
Greitzer, Frank L. 2019. "Insider Threats: It's the HUMAN, Stupid!" In Proceedings of the Northwest Cybersecurity Symposium, 1–8. NCS '19. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/3332448.3332458.
[16] Dawn Cappelli, Andrew P. Moore, and Randall F. Trzeciak. The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud). 2012. https://insights.sei.cmu.edu/library/the-cert-guide-to-insider-threats-how-to-prevent-detect-and-respond-to-information-technology-crimes-theft-sabotage-fraud/
Keeney, Michelle & Kowalski, Eileen & Moore, Andrew & Shimeall, Timothy & Rogers, Stephanie. (2005). Insider threat study: Computer system sabotage in critical infrastructure Sectors. SEI CERT: Carnegie Mellon University.
[17] Serenko, "Knowledge Sabotage."

seek to gain a competitive advantage over others at work or seek revenge for interpersonal or organizational grievances.[18]
    - Hiding valuable information from coworkers, for example, gives individuals near-exclusive access to necessary work-related information and places them in a position of relative power to others who must then rely on the knowledge holders (i.e., brokers) for information.[19]
- Situations that fuel retaliatory acts of sabotage may include customer mistreatment,[20] interpersonal conflict at work,[21] and frustration or ethical conflict with one's work and organization.[22]
- Taken together, most insider sabotage events arise from self-gratification or retribution motives, but the nature of actions taken hinges on the insider's access to critical organizational resources and capacity to thwart organizational processes.



Case Study: Mittesh Das

- In November of 2014, a national-level computer program responsible for handling pay and personnel actions for U.S. Army reservists began experiencing unusual issues. Standard internal troubleshooting uncovered suspicious code that led to an investigation by the Army's Criminal Investigation Command.
- The investigation revealed that in 2012, due to his vast experience with the system, the contracted company responsible for oversight of the system had subcontracted with Das to assume lead responsibility. However, the contract was set to be awarded to a new company, with a handoff in November of 2014.

---

[18]Serenko, Alexander, and Chun Wei Choo. 2020. "Knowledge Sabotage as an Extreme Form of Counterproductive Knowledge Behavior: The Role of Narcissism, Machiavellianism, Psychopathy, and Competitiveness." Journal of Knowledge Management 24 (9): 2299–2325. https://doi.org/10.1108/JKM-06-2020-0416.
Crino, "Employee Sabotage."
Gruys, Melissa L., and Paul R. Sackett. 2003. "Investigating the Dimensionality of Counterproductive Work Behavior." *International Journal of Selection and Assessment* 11 (1): 30–42. https://doi.org/10.1111/1468-2389.00224.
[19] Kwon, Seok-Woo, Emanuela Rondi, Daniel Z. Levin, Alfredo De Massis, and Daniel J. Brass. 2020. "Network Brokerage: An Integrative Review and Future Research Agenda." *Journal of Management* 46 (6): 1092–1120. https://doi.org/10.1177/0149206320914694.
Perotti, Francesco Antonio, Alberto Ferraris, Elena Candelo, and Donatella Busso. 2022. "The Dark Side of Knowledge Sharing: Exploring 'Knowledge Sabotage' and Its Antecedents." Journal of Business Research 141 (March): 422–32. https://doi.org/10.1016/j.jbusres.2021.11.033.
[20] Harris, Lloyd C., and Emmanuel Ogbonna. 2006. "Service Sabotage: A Study of Antecedents and Consequences." *Journal of the Academy of Marketing Science* 34 (4): 543–58. https://doi.org/10.1177/0092070306287324.
Skarlicki, Daniel P., Danielle D. van Jaarsveld, and David D. Walker. 2008. "Getting Even for Customer Mistreatment: The Role of Moral Identity in the Relationship between Customer Interpersonal Injustice and Employee Sabotage." *The Journal of Applied Psychology* 93 (6): 1335–47. https://doi.org/10.1037/a0012704.
[21] Eissa, Gabi, and Rebecca Wyland. 2016. "Keeping up with the Joneses: The Role of Envy, Relationship Conflict, and Job Performance in Social Undermining." *Journal of Leadership & Organizational Studies* 23 (1): 55–65. https://doi.org/10.1177/1548051815605020.
[22] Ambrose, Maureen L, Mark A Seabright, and Marshall Schminke. 2002. "Sabotage in the Workplace: The Role of Organizational Injustice." *Organizational Behavior and Human Decision Processes* 89 (1): 947–65. https://doi.org/10.1016/S0749-5978(02)00037-7.

- Shortly before the handoff, Das inserted malicious code - commonly referred to as a "logic bomb" – in the days leading up to a contract changeover and that the progressively destructive nature of this code began taking effect the day after the changeover.
- In 2017, a federal jury found Das guilty of knowingly transmitting malicious code with the intent to cause damage to a U.S. Army computer used in furtherance of national security.[23]

Lessons from Political Violence Research

Although violent extremist beliefs are of concern, the foundations of politically motivated violent actions

- Extremist insiders are particularly concerning not only for the potential of political violence but for the risk of ideologically motivated insider attacks, which is especially concerning for those radicalized after hiring.
    - For example, a federal employee who begins adhering to Anti-Government Anti-Authority Violent Extremism (AGAAVE) has the potential to cause significant harm depending on their access.
- Researchers are still working to understand what distinguishes those who engage in violence from other, nonviolent ideological extremists.
- What is increasingly clear is that it is **not static factors** that best predict the risk of violence, but rather, **dynamic ones**. For example, fixed traits such as race, nationality, age, and sex by themselves are poor predictors of violence, regardless of an individual's level of extremism.
    - Rather, how people interact with their sociopolitical environments better explains their violence risk.[24]
        - For instance, while Racially and Ethnically Motivated Violent Extremism (REMVE) attackers have accounted for most of the recent domestic violent extremism (DVE) attacks in the United States, AGAAVE attackers pose a greater risk to law enforcement and other authority figures resulting from situational interactions such as traffic stops.[25]
        - Such differences between these violent extremists suggest that discrete triggering events or contexts, in combination with one's beliefs, can increase the perceived viability and likelihood of violent behavior.[26]
    - This parallels with lessons from espionage—that is, triggering event aligns with opportunity and individual personality pathologies such as thrill-seeking behavior for an act of espionage to occur.
    - Additionally, group norms and membership can convince those with grievances and aggressive tendencies (or even those without, who join groups and movements out of social

[23] "Eastern District of North Carolina | Georgia Man Sentenced for Compromising U.S. Army Computer Program | United States Department of Justice." 2018. September 11, 2018. https://www.justice.gov/usao-ednc/pr/georgia-man-sentenced-compromising-us-army-computer-program.
[24] Neo, Loo Seng, Leevia Dillon, and Majeed Khader. 2017. "Identifying Individuals at Risk of Being Radicalised via the Internet." *Security Journal* 30 (4): 1112–33. https://doi.org/10.1057/s41284-016-0080-z.
[25] Clifford, Bennett; Program on Extremism, George Washington University; and National Counterterrorism Innovation, Technology, and Education Center, "RACIALLY/ETHNICALLY MOTIVATED VIOLENT EXTREMIST (RMVE) ATTACK PLANNING AND UNITED STATES FEDERAL RESPONSE, 2014-2019" (2021). Reports, Projects, and Research. 11. https://digitalcommons.unomaha.edu/ncitereportsresearch/11
Strategic Intelligence Assessment and Data on Domestic Terrorism. (2021). [File]. Federal Bureau of Investigation. Retrieved October from https://www.fbi.gov/file-repository/fbi-dhs-domestic-terrorism-strategic-report.pdf/view
[26] Hamm, M., & Spaaj, R. (2015). Lone Wolf Terrorism in America: Using Knowledge of Radicalization Pathways to Forge Prevention Strategies. U.S. Department of Justice.

pressure or solidarity) to justify their mobilization toward violence for social and political aims.[27]

- Political beliefs can also be used to justify a range of potential insider harms and are a common motive for many espionage and sabotage cases. Consider the hacktivism[28] group Anonymous. Most recently, Anonymous has been in the news for attacking Russian computer systems in protest of the 2022 Russian Invasion of Ukraine.[29]
    - Edward Snowden, charged with multiple espionage statutes in 2013 for mass leakage, defended his actions, saying they were "to inform the public as to that which is done in their name and that which is done against them."[30]
    - While many hackers breach protected information to sell personal data for profit, others are ideologically motivated, and the two often intertwine.
        - Cases like Snowden and Anonymous underline the shifting nature of both technology and an increasingly globalized world, as well as how they impact espionage and insider threats.
    - Thus, although violent extremist beliefs are of concern, the foundations of politically motivated violent actions are often *also* social or contextual.

Case Study: 2009 Fort Hood Shooting

- On November 5th, 2009, Nidel Hassan, an Army Major and psychiatrist, opened fire at the Fort Hood Military base near Killeen, Texas.[31]
- He fatally shot 13 and left another 30 injured, while he sustained injuries that left him paralyzed from the waist down.
- Many consider it a terrorist attack due to Hassan's increasingly radical beliefs, describing him as a homegrown violent extremist.[32] Others view the attack as a case of workplace violence.[33] The subject remains controversial to this day.

Lessons from Organizational Psychology Research

- Insider threats can stem from unintentional (e.g., human or system error) or intentional (i.e., malicious) sources.
- Workplace misbehavior often stems from personal factors (e.g., deviant personalities, personal interests that mismatch with organizational interests), interpersonal grievances or social

[27] Asal, V., Schulzke, M., & Pate, A. (2017). Why do some organizations kill while others do not: An examination of Middle Eastern organizations. Foreign Policy Analysis, 13(4), 811-831. http://dx.doi.org/10.1111/fpa.12080
Clifford, Bennett, and Jon Lewis. 2022. "'This Is the Aftermath': Assessing Domestic Violent Extremism One Year After the Capitol Siege." Washington: Program on Extremism at George Washington University. https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/This%20is%20the%20Aftermath.pdf
[28] Hacking to achieve social action of political objectives.
[29]Rounak, J. (2022). Russia-Ukraine war: Anonymous hackers launch cyberwar against Russia taking down government websites. Business Insider. https://www.businessinsider.in/tech/news/russia-ukraine-war-anonymous-hackers-launch-cyberwar-against-russia-taking-down-government-websites/articleshow/89817168.cms
[30] Greenwald, G., MacAskill, E., & Poitras, L. (2013). Edward Snowden: The whistleblower behind the NSA surveillance revelations. The Guardian. https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance
[31] Soldier Opens Fire at Ft. Hood; 13 Dead—CBS News. (2009). Retrieved from https://web.archive.org/web/20131005013430/http://www.cbsnews.com/stories/2009/11/05/national/main5539067.shtml
[32] News, A. B. C. (2012). Fort Hood Victims Demand Attack Be Deemed "Terrorism." ABC News. Retrieved from https://abcnews.go.com/Blotter/fort-hood-victims-demand-attack-deemed-terrorism/story?id=17525656
[33] Meleagrou-Hitchens, A. (2015, September 24). Jihad in the Workplace: Looking Back on the Fort Hood Shooting. War on the Rocks. https://warontherocks.com/2015/09/jihad-in-the-workplace-looking-back-on-the-fort-hood-shooting/

contagion, or organization factors (e.g., unfair policies, pay inequity, overwork), and be directed at employees or the organization.
- Intentional harm to the organization can involve forms of information, process, or infrastructure sabotage.

Interpersonal Aggression and Violence at Work

- Intentional harm to people can range from workplace aggression (behaviors such as bullying or incivility that cause, or are intended to cause, psychological harm) to workplace violence (attempts to physically harm others in the workplace).[34]
- Unlike most insider threat research, research on workplace aggression and workplace violence also extends to non-employee perpetrators such as customers or others who might gain entry into the organization.
- Workplace violence research distinguishes among four types of workplace violence that vary by the relationship between the perpetrator and the organization:[35]
    - **Criminal Intent.** In this type of workplace violence, the perpetrator has no legitimate relationship with the organization and is perpetuating violence as part of a criminal motive, such as robbery.
    - **Customer**. In this type of workplace violence, the perpetrator is a client, customer, student, or other similar status. Thus, the perpetrator has a legitimate relationship with the organization but is not considered part of the organization.
    - Employee. This type of workplace violence is perpetrated by a current or former employee and would typically be considered an "insider threat."
    - **Personal Relationship**. In this type of workplace violence, the perpetrator has a relationship or association with someone in the organization, but not the organization itself. Often these are domestic disputes that carry over to the workplace context.
- Workplace violence is rare and influenced by work settings. For example, criminal and customer workplace violence is most likely to occur in organizations that interface regularly with the public.[36]

Workplace violence is rare and influenced by work settings. For example, criminal and customer workplace violence is most likely to occur in organizations that interface regularly with the public.

Workplace Violence Offender Characteristics

- Piquero and colleagues[37] found that behavioral and attitudinal risk factors for workplace violence include (a) motives for violence, (b) homicidal fantasies/violent preoccupations, (c) weapon skill/access/involvement, (d) preattack planning and preparation, and (e) suicidality/depression.
- Geck and colleagues[38] performed one of few empirical studies that distinguished between individual risk factors for aggression versus violence in a workplace setting. Compared to aggressive non-

[34] Geck, Celia M., Teresa Grimbos, Maurice Siu, Philip E. Klassen, and Michael C. Seto. 2017. "Violence at Work: An Examination of Aggressive, Violent, and Repeatedly Violent Employees." *Journal of Threat Assessment and Management* 4 (4): 210–29. https://doi.org/10.1037/tam0000091.
[35] "Workplace Violence Prevention Strategies and Research Needs." 2006. U.S. Department of Health and Human Services, Public Health Service, Centers for Disease Control and Prevention, National Institute for Occupational Safety and Health. https://doi.org/10.26616/NIOSHPUB2006144.
Cybersecurity and Infrastructure Security Agency (CISA) (2019). Violence in the federal workplace: A guide for prevention and response (Version 4.0). Interagency Security Committee. Retrieved from https://www.cisa.gov/resources-tools/resources/isc-violence-federal-workplace-guide
Geck, et al., "Violence at Work."
[36] Piquero, Nicole Leeper, Alex R. Piquero, Jessica M. Craig, and Stephen J. Clipper. 2013. "Assessing Research on Workplace Violence, 2000–2012." *Aggression and Violent Behavior* 18 (3): 383–94. https://doi.org/10.1016/j.avb.2013.03.001.
[37] Piquero, et al., "Assessing research on workplace violence."
[38] Geck, et al., "Violence at Work."

violent cases, they found that violent individuals were (a) more likely to have a marital status, potentially suggesting a spillover effect from home, (b) less likely to have been formally diagnosed with a mental illness, (c) less likely to have a history of threats, but more likely to have a history of violence in the workplace.

Worker-on-Worker Violence Deterrence and Management Strategies

- ***Ethical workplace leadership, culture, and practices.*** Insider threat mitigation programs can be improved using positive deterrence strategies, which focus on aligning employee interests with organizational interests.[39] Unlike punitive command-and-control security practices aimed at reducing deviance, positive deterrence may involve leaders' role-modeling of ethical behaviors, building supportive work cultures that increase employee rapport and collaboration, and fair workplace policies and practices that meet employee interests.
- ***Screening processes to select out individuals at an elevated risk of committing violence.*** This includes implementing pre-employment vetting processes (e.g., reference checks) and making use of probationary periods.
- ***Training programs to protect the workforce from potential violence***. This includes training for employees (e.g., on policies and procedures, as well as prevention strategies, such as anger and stress management), supervisors, and incident response teams.
- ***Alternative Dispute Resolution (ADR) programs***. ADR is an umbrella term for resolving disagreements through a neutral third party, such as ombudsmen, facilitation, and mediation.
- ***Incident response or threat assessment teams.*** Summarizing current promising practices for workplace threat assessment teams specifically is beyond the scope of the current section but is a critical element in workplace violence prevention.
- ***Employee Assistance Programs (EAPs).*** EAPs can be critical to early intervention efforts.
- ***Processes to help organizations recover after an incident.*** This involves the identification of trained mental health professionals and the deployment of procedures (e.g., the Psychological First Aid model) to assist with recovery.

Grant Acknowledgement and Disclaimer: This material is based upon work supported by the U.S. Department of Homeland Security under Grant Award Number 70RSAT21G00000002/70RSAT21FR0000084. The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security or the University of Nebraska at Omaha.

[39] Moore, Andrew P., Carrie Gardner, and Denise M. Rousseau. 2022. "Reducing Insider Risk Through Positive Deterrence." *Counter-Insider Threat Research and Practice* 1 (1). https://citrap.scholasticahq.com/article/34612-reducing-insider-risk-through-positive-deterrence.