

DOI:10.1145/3408864

Tracing the relationship between pathological personality traits and insider cyber sabotage.

BY MICHELE MAASBERG, CRAIG VAN SLYKE,
SELWYN ELLIS, AND NICOLE BEEBE

The Dark Triad and Insider Threats in Cyber Security

“I WAS DISMAYED to learn this weekend about a Tesla employee who had conducted quite extensive and damaging sabotage to our operations. This included making direct code changes to the Tesla Manufacturing Operating System under false usernames and exporting large amounts of highly sensitive Tesla data to unknown third parties.”

—Tesla CEO Elon Musk in an email to Tesla employees.⁶

Insider cyber sabotage⁴ such as that mentioned by Mr. Musk is one of the reasons cyber security remains a top managerial concern. Insider threats, such as the Tesla sabotage, are among the greatest of these security concerns.²⁴ A major reason for this is that insider security breaches are seen as more costly than those from outsiders.^{16,20}

Understanding the individual, social, and organizational influences on insider threats is important to the development of security-related policies and controls. Cyber sabotage as part of a broader insider threat issue is addressed in the context of an organizational security risk management plan. Such plans should include security controls intended to mitigate the risk of a human threat from the inside. In the U.S., in some cases in which classified material is involved, formal insider threat cyber security programs are mandated by Presidential Executive Order.

The security controls prescribed by insider threat programs often include automated employee monitoring systems for detection, education and training programs for awareness.⁹ These controls often include technical and behavioral indicators derived from the observed psychological traits and specific behaviors of high-risk insiders. These indicators should be based on empirical evidence in order to avoid false accusations that harm employees⁷ and negative ethical and legal consequences associated with biased systems.¹²

Insiders possess unique personal predispositions, stressors, and concerning behaviors that have been identified as risk factors; these have been included in models of insider threat behaviors.^{8,18} Past research suggests that robust cybersecurity systems include psychological or personality factors in their design.⁹ Several insider threat frameworks include personal predispositions (including personality traits) as the origin point of threat behaviors.^{8,17,18} This suggests it is important to recognize personal factors, especially personality traits, before

» key insights

- **Malicious insider threats often exhibit the malevolent personality traits subclinical narcissism, psychopathy, and Machiavellianism known as the dark triad.**
- **The cost of hiring a toxic worker typically exceeds any benefit that they might bring to an organization.**

IMAGE BY ALICIA KUBISTA/ANDRIJ BORYS ASSOCIATES




they lead to malicious behaviors. Such recognition can be the earliest point of threat agent identification.

Much of the existing research into personality traits and cybersecurity is based on case studies, anecdotal evidence, or conceptual reasoning. There is a lack of quantitative empirical evidence to guide our understanding of the relationship between personality traits and insider threats.¹³ Understanding the role of traits related to antisocial behavior in malicious insider threats is especially important due to the link between these traits and malevolent behavior. The findings of our research may help enhance and extend existing models and frameworks including advanced technical systems.


In this article, we focus on a set of pathological personality traits known as the dark triad. Evidence from recent insider threat cases leads us to believe these traits may correlate with intentions to engage in malicious behavior.²³ After discussing insider threats and the dark triad traits, we present results from an empirical study that illustrate the relationship between the dark triad traits and malicious intent. We then discuss the importance of these results and make recommendations for security managers and practitioners based on our findings. Despite the inclusion of personality traits in insider threat frameworks, to our knowledge no known studies have empirically investigated the relationships between the dark triad traits (individually or collectively) and insider cyber sabotage. The findings of our research may help enhance and extend existing models and frameworks of insider threat behavior. Additionally, the findings may contribute to empirically validating rulesets in technical systems and traits used in insider threat training and awareness programs.

Background

Insider threats. Insiders represent greater threats to organizations than outsiders due to their access to organizational information and information systems, especially when coupled with their advanced organizational knowledge and the trust that is often afforded to them. Insider threats exist when trusted current or former organizational members act in ways that expose the organization to risk.⁹ Inappropriate insider behavior not only threatens orga-



Machiavellians engage in bad behaviors for some gain, narcissists engage in bad behaviors because they are only concerned with themselves, and psychopaths behave badly for the thrill, regardless of the risk to themselves or an organization.



nizational resources, it may put the survival of the organization at risk.

When discussing insider threats, it is useful to distinguish between malicious and unintentional threats. Not surprisingly, the key difference is intent. Unintentional threats come from actions (or inactions) undertaken without any malicious intent. Using an easy-to-guess password or responding to a phishing email are examples of unintentional threats. In contrast, malicious threats come from intentional acts. The CERT National Insider Threat Center (NITC) defines a malicious insider threat as “a current or former employee, contractor, or business partner who has or had authorized access to an organization’s network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization’s information or information systems.”²² The research presented here pertains to malicious, rather than unintentional, insider threats.

Malicious insider threats are often described by the nature of the crime or abuse.⁷ For example, a common categorization of malicious insider threats includes espionage, cyber sabotage, fraud, and theft of intellectual property.^{1,20} Cyber sabotage, or the infliction of harm on some area of an organization using technology,^{4,20} can result in particularly significant and diversified damage to that organization.⁵

There are numerous methods for dealing with the threat of insider sabotage. These include technical and administrative preventive and deterrent mitigation techniques. Technical approaches include user and enterprise level systems for detection focusing on monitoring of cyber data.⁹ These systems include capabilities for collection, storage, analysis, and reporting based on activities and actions of individuals. Administrative controls include training and awareness programs, security policies, and processes that include securing system access paths upon precipitating events, such as demotion or termination.²⁰ Our research can be used to enhance both technical and administrative approaches, as discussed later.

Personality factors, particularly pathological personality traits, have been cited as one of three essential factors predisposing individuals to mali-

cious insider threat behavior (along with opportunity and states of crisis).²³ Past insider threat cases have noted key personal predispositions as precursors to espionage and cyber sabotage. These predispositions include an unusual need for attention, sense of entitlement, arrogance, impulsivity, lack of conscience, and lack of empathy.¹ These key characteristics reported of convicted insiders are also elements of the dark triad of personality.

The underlying psychology of individual threat agents lies at the heart of the insider threat problem. Although technical controls are helpful in mitigating harmful behaviors, they are insufficient. As experience repeatedly demonstrates, insider threat behaviors occur in spite of sophisticated technical security mechanisms. One reason for this is that these mechanisms typically detect threat activity only after the activity occurs. In addition, clever bad actors are often able to circumvent technical security controls. On the other hand, common administrative controls such as security policies and associated sanctions may not account for the underlying psychology of malevolent individuals. As we explain later, such individuals may ignore policies and be unmoved by the risks associated with potential sanctions. Because of this, it is important to understand the traits of atypical, malevolent insiders. Thus, neither technical nor administrative controls alone can address the malicious insider threat problem. There needs to be an advanced holistic approach that considers insiders' psychological factors. Fair and trustworthy algorithms to support the advanced systems depend on empirical evidence derived from rigorous studies.

Dark triad. There are numerous models of personality. Perhaps the most commonly known is the five-factor model, which consists of five constructs of personality that are robust across cultures.² However, according to some, the five-factor model fails to fully account for individual differences in personality-related behaviors, particularly when related to antisocial behaviors.²² Recent research addresses this weakness by adding traits that represent socially malevolent behavior. The dark triad of personality represents a set of personality characteristics that are only partially accounted for by the five-factor model.²²

The dark triad consists of three socially aversive personality traits—Machiavellianism, narcissism, and psychopathy.¹⁵ All three of these exhibit a socially malevolent character: self-promotion, emotional coldness, duplicity, and aggressiveness. However, the three traits exhibit these tendencies to different degrees. Further, all three are to some extent manipulative, Machiavellianism most markedly so. Machiavellianism is a manipulative personality characterized by interpersonal relationship strategies oriented toward manipulation, self-interest, and deception. Those with Machiavellian personalities are primarily concerned with self-interest and are typically unconcerned about others beyond how they can serve that self-interest. Not surprisingly, Machiavellianism is negatively correlated with empathy. Narcissism is characterized by a general sense of superiority, grandiosity, entitlement, and dominance. Narcissists focus on themselves and have an inflated self-view. As is the case with Machiavellianism, narcissism is negatively correlated with empathy. Psychopathy is characterized by an arrogant, deceitful approach to relationships, along with high impulsivity and thrill-seeking, and irresponsible behavior. In addition, psychopathic personalities are deficient in affect, and exhibit low empathy and low anxiety.

Table 1 summarizes key characteristics the dark triad personalities.

While all three dark triad personalities are socially malevolent, they differ in how social interactions and others are viewed. All three are unconcerned with any potential negative impacts their behaviors may have on others. Machiavellians seem to be concerned about how they can manipulate and use others to achieve personal goals, without consideration of how others might be negatively affected. Machiavellians will manipulate and exploit others, but with some goal in mind. If the manipulation and exploitation is unlikely to advance the Machiavellian's goal, the Machiavellian is unlikely to bother.

Narcissists are highly self-focused. They will engage in malevolent behavior, but that behavior may be due to the narcissist's sense of grandiosity, entitlement, and superiority rather than an explicit desire to do harm or negatively impact others. Narcissists do not care about impacts on others because they view others as unimportant. Narcissists are less likely than Machiavellians or psychopaths to consciously engage in behavior that harms others. Narcissists engage in such behaviors because they do not think of others.

A more complex set of factors lead to malevolent behaviors among those with psychopathic personalities. These

Table 1. Dark Triad traits.^{1,11,15,22}

Key Characteristics	Machiavellianism	Narcissism	Psychopathy
Duplicity	×	×	×
Self-promotion	×	×	×
Aggressiveness	×	×	×
Interpersonal coldness	×	×	×
Tendency to manipulate and exploit others	×	×	×
Sense of superiority	×	×	×
Low empathy	×	×	×
Callousness/lack of conscience	×	×	×
Attention to reputation	×	×	
Cynical world view	×		
Strategic calculation	×		
Sense of entitlement		×	
Sense of grandiosity		×	
Ego-reinforcement all-consuming motive		×	
Thrill-seeking			×
Low anxiety			×
Lack of impulse control			×

individuals are not focused on the end goal that drives the Machiavellian. They engage in malevolent behavior for the thrill. Further, due to their low levels of anxiety they are not concerned about “getting caught.” These factors, when combined with deficient affect and low empathy, make for a dangerous combination. To summarize, **Machiavellians engage in bad behaviors for some gain, narcissists engage in bad behaviors because they are only concerned with themselves, and psychopaths behave badly for the thrill, regardless of the risk to themselves or an organization.**

Dark triad personality traits can predict and explain workplace behavior.¹⁰ This thinking has been applied after the fact to explain insider threat incidents. Numerous insiders involved in well-known threat cases displayed personality traits similar to those included in the dark triad. While not labeled as such, current insider threat research identifies several dark triad traits as being related to insider threats, including a sense of entitlement and lack of empathy.¹⁹ However, to date no known study has used the dark triad as a framework for examining insider cyber sabotage.

Despite the emergence of dark triad personality traits in insider threat cases, there is a lack of systematic empirical research into the relationship between personality traits and insider threat behavior. Our study addresses this issue by empirically demonstrating the link between dark triad traits and intentions to engage in an insider threat behavior (cyber sabotage).

Methods and Results

The study was conducted using the Amazon Mechanical Turk (MTurk) marketplace to deploy an experimental vignette to a sample of working professionals from a variety of technology, healthcare, manufacturing, finance, academic, and service-oriented organizations. The vignette described an event in which an employee, who had recently been denied

a raise, accessed a restricted database that had been left open inadvertently and discovered that several peers had 20% higher salaries than the employee. The employee copied the database and posted it to the company’s website. Subjects were asked to put themselves in the place of the employee when answering questions regarding the sabotage performed by the employee. A total of 768 usable observations were obtained after removing cases with missing data. The participants ranged in age from 18 to 73 years, with mean age of 34.7 years. The sample was 42% female and 58% male. All participants were employed, with a mean tenure in their current position of 6.08 years.

We used previously validated scales to measure the dark triad traits¹¹ and a previously validated scale for revenge, which was adapted to the vignette, to measure intentions.³ All scale items were measured on a seven-point scale. The relationships were tested using Mplus Version 7 software to run covariance based latent variable modeling using weighted least squares means and adjusted variances (WLSMV) estimation for categorical data using a polychoric correlation matrix. All fit indices met the minimum requirements for interpretations of results. Validity and reliability were satisfactory.

The results of model testing showed that the relationships between each of the dark triad traits and intentions to engage in insider threat behavior were positive and significant, as shown in Table 2. The strength of the relationships varied across the traits. Psychopathy had the strongest relationship ($\beta = 0.559$, $p < 0.001$), followed by Machiavellianism ($\beta = 0.379$, $p < 0.001$) and narcissism ($\beta = 0.286$, $p < 0.001$).

To further examine the relationship between the dark triad and intent, we created an index of the dark triad by computing a mean of an individual’s score on all three traits. For example, an individual who scored five on Machiavellianism, a four on psychopathy, and a

three on narcissism had a dark triad score of four. This measure gives a more holistic view of the relationship between the dark triad concept and malevolent intent. After we computed the dark triad index score, we prepared a scatter plot with intent on the x -axis and the dark triad index score on the y -axis. Then we used color to represent the psychopathy score, and symbol size to indicate the Machiavellianism score. Narcissism is shown by the three symbols; with high, moderate, and low narcissism scores shown by the circle, plus sign, and square respectively. We defined the three different levels according to the scores distance from the mean, with plus or minus one standard deviation from the mean being high and low respectively.

The right-hand side of the plot may be thought of as the *danger zone*, as these individuals are above the intention midpoint. There is an interesting contrast between the lower- and upper-right quadrants. The lower-right quadrant is the least populated quadrant. One interpretation of this is that, generally speaking, those who have low dark triad scores are unlikely to have malevolent intentions. Further, no individual with a dark triad score of less than approximately 1.75 is on the higher end of the intent scale. In contrast, the upper-right quadrant has numerous circles. Circles in this quadrant are relatively large, indicating high Machiavellianism scores, and tend to be red, rather than blue, indicating relatively high psychopathy scores. Taken together, these results seem to indicate meaningful relationships between dark triad scores and intention to commit insider cyber sabotage.

We must caution that this visual analysis is exploratory. To our knowledge, there is no established method for creating a formal dark triad score. Further, there is no theoretically or empirically established rationale for causal relationships among the dark triad traits. For these reasons, we are reluctant to perform statistical tests on the relationship between dark triad scores and intentions; such tests may imply a higher level of precision that we can claim.

Discussion

Our results clearly show the link between the dark triad and intentions to engage in malicious insider threat behavior. While there are strong, positive relation-

Table 2. Results.

Dark Triad Trait	Beta	P-value
Machiavellianism	0.379	< 0.001
Narcissism	0.286	< 0.001
Psychopathy	0.559	< 0.001

ships between each of the three dark triad traits and intentions, the strength of the relationships varied across the traits. Psychopathy had the strongest relationship, followed by Machiavellianism and narcissism. In this section, we discuss these results, including implications, recommendations for practice, and avenues for future research.

Before discussing our results, it is important to understand that the presence of dark triad traits is only one potential precursor to insider threat behavior. A sound cybersecurity risk assessment system should include assessing the dark triad traits along with other individual and organizational factors.⁹ The presence of dark triad traits, when found with these other factors, increases risk.

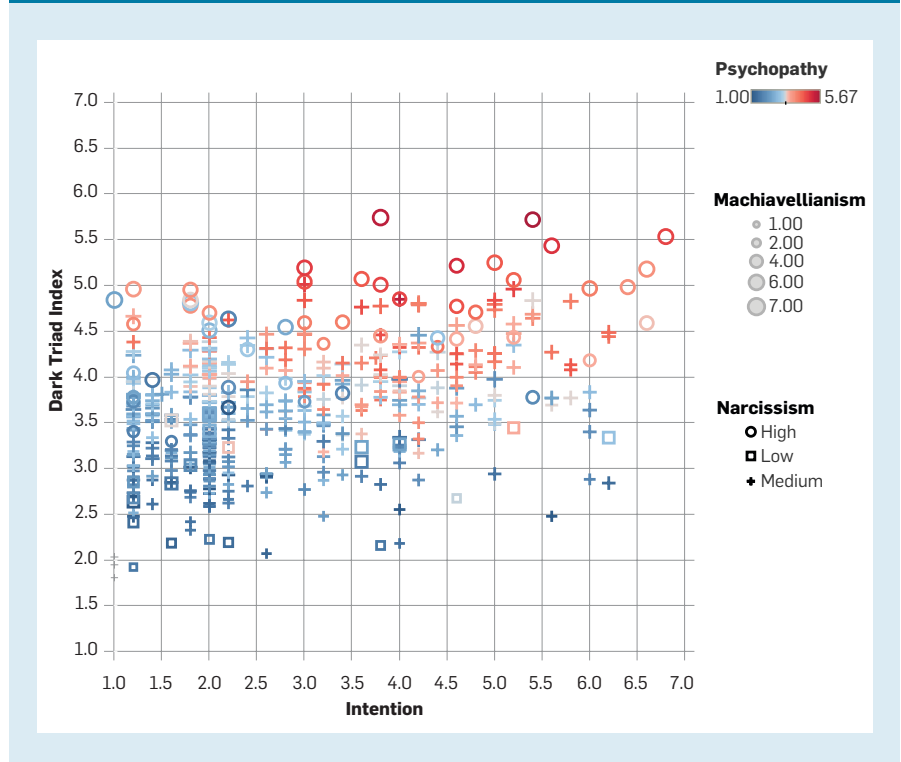
Our research answers the call for empirical validation of precursors of insider threats⁹ by providing evidence of the relationship between specific personality traits and cyber sabotage. Numerous frameworks, guidelines and awareness campaigns include personal characteristics, which demonstrates the importance of personality in cyber security risk management. However, there has been a lack of empirical evidence that can be used to guide the understanding of specific concerning personality types. The empirical evidence provided in this study should be useful for refining existing cybersecurity resources related to insider threats and refine indicator development in technical monitoring systems.

There is considerable good in organizations; most individuals are hard-working and ethical. However, our research shows that individuals who tend toward the dark triad traits are more likely to intend to engage in harmful behaviors. Hence, managers should be aware of the traits and the associated tendencies toward harmful behaviors. Further, managers should have some understanding of how to deal with the threats brought about by insiders who exhibit dark triad traits.

Recommendations

Overall, managers can be thankful for the good in their organizations and for their hard working, principled employees. However, some individuals will tend toward malevolent personality traits. Because of this, developing and employing risk management strategies directed at mitigating the potential harm these indi-

Figure 1. Dark triad index and insider cyber sabotage intention scatterplot.



viduals may bring is important. Employing such strategies is important due to the grave damage these individuals can do through their access to information assets and systems. Our data show that most employees are not inclined toward malevolent personality traits or malicious behaviors. However, as Figure 1 illustrates, malevolent people do exist, and those individuals are significantly more likely to intend to use information technology systems to do harm. These individuals are dangerous—managers should be aware of the dangers they pose.

Both administrative and technical techniques exist for mitigating the potential harm from insiders. Although the following recommendations focus on administrative controls, technical controls are equally important. Our research pertains to both administrative and technical controls. The results can provide guidance for developing and refining policy, training and awareness programs, and technical monitoring systems. All of these are important elements of a well-designed cybersecurity risk management system.

Educating managers on the dark triad traits may help them identify high-risk individuals, which is an important administrative mitigation technique. Strong hiring practices that include

thorough screening through multiple interviews and pre-employment testing¹⁴ may help avoid hiring high-risk individuals. The costs of bad hires significantly exceed the potential benefits they may bring an organization, even if these individuals are “superstars.”²¹ Hiring managers should follow the medical community’s credo, *primum non nocere*, first do no harm,²¹ and actively avoid hiring high-risk insiders.

Even the most stringent hiring practices may not prevent hiring malicious individuals. Because of this, a well-designed risk management plan should assume that high-risk insiders exist in the organization and should seek to identify such individuals. However, it is important that such practices not be illegally discriminatory. Balancing the line between prudence and practices that may be seen as discriminatory requires careful thought and planning, along with the involvement of human resource and legal specialists.⁴ This can be accomplished by implementing issue-specific administrative-preventative security policies as part of an overall risk mitigation plan. Many organizations have formal processes in place for insider threat cases, and if staff is well trained, behavioral patterns associated with threats resulting from the personality traits can be

recognized sooner, with formal risk-management processes triggered.⁴

Sound leadership practices may help mitigate the risk from malevolent insiders. For example, psychopathic or Machiavellian individuals who perceive that some people (such as managers) are allowed to break rules that others must follow may seek revenge through the misuse of information assets. Broken promises (real or perceived) may also trigger adverse behavior in those high in dark triad traits. For example, such individuals may be motivated to do harm when a promised bonus, raise, or promotion does not come to pass. The motivation may be even stronger when the promised benefit is given to someone else.


We would be remiss if we did not mention the clear ethical dilemma posed by our recommendations. Managers face a trade-off between their responsibility to protect the organization and the rights of current and potential employees. This trade-off is similar to that presented in employee monitoring, which requires balancing organizational risk and employee privacy.¹² Hence, we consider the use of personality traits as elements of screening or monitoring efforts because assessment devices have been designed for use in normal populations and there is no reason to believe the individuals are clinically impaired regarding critical functions of the job for which they were hired.²⁵

Limitations and directions for future research. This study has limitations that provide future research opportunities. First, the study confirmed a relationship but was limited in the ability to establish full causality. Due to limitations with the temporal precedence criterion, only association can be concluded. Future research using laboratory experimental or longitudinal methods are called for. Second, the generalizability of our findings is limited by our use of a specific scenario that included a particular trigger and threat. Future research should consider a range of scenarios that include additional triggering events and threat responses.

One particularly important open question concerns the effectiveness of commonly used deterrents. Some common deterrents such as sanctions may not only be ineffective for psycho-

paths—the risk associated with the deterrent may actually be a motivator. It is likely that what management perceives as deterrents may not be viewed as such by malevolent individuals. Another important goal for future research is to gain a better understanding of what motivates individuals high on the dark triad traits to engage in harmful behaviors. Are there particular events that lead dark triad individuals to engage in malevolent behaviors? A related question concerns how the dark triad traits influence cybersecurity decision making. Finally, researchers should seek to understand the extent to which dominant behavioral security theories apply to those exhibiting the dark triad traits, particularly in the context of malicious insider cyber security threats.

Conclusion

This study establishes the relationships between dark triad personality traits and intentions to commit insider cyber sabotage. We found strong, significant relationships between the dark triad traits and such intentions. Dark triad individuals have a propensity toward malicious insider threat acts. Although it is ideal to avoid hiring individuals exhibiting high risk traits, the difficulty in identifying such individuals during the hiring process means that they likely exist in most organizations. When it comes to malicious insider threat risk mitigation, a false positive is much better than a false negative. 

Acknowledgments

Financial support was provided by the Dr. Jan Clark Memorial Research Fund and the Herbert McElveen Professorship made available through the state of Louisiana Board of Regents Support Funds and Mary Nell Condren.

References

1. Band, S.R., Cappelli, D.M., Fischer, L.F., Moore, A.P., Shaw, E.D. and Trzeciak, R.F. Comparing Insider IT Sabotage and Espionage: A Model-Based Analysis. Technical Report #CMU/SEI-2006-TR-026. Carnegie Mellon University Software Engineering Institute Pittsburgh, PA.
2. Barrick, M.R. and Mount, M.K. The big five personality dimensions and job performance: A meta-analysis. *Personnel Psychology* 44, 1 (1991), 1–26.
3. Bradfield, M. and Aquino, K. 1999. The effects of blame attributions and offender likableness on forgiveness and revenge in the workplace. *J. Management* 25, 5 (1999), 607–631.
4. Cappelli, D. An unaddressed threat to critical infrastructure and national security: Insider cyber sabotage. 2018; <https://bit.ly/2CpdphW>.
5. Clark, J.W. Threat from within: Case studies of insiders who committed information technology sabotage. In *Proceedings of the 11th Intern. Conf. Availability, Reliability and Security* (Salzburg, Austria, Aug. 2016), 414–422.
6. CNBC. Elon Musk emails employees about “extensive and damaging sabotage” by employee. 2018; <https://cnb.cx/2YnYgGr>.

7. Greitzer, F.L., Frincke, D.A. and Zabriskie, M. Social/ethical issues in predictive insider threat monitoring. *Information Assurance and Security Ethics in Complex Systems: Interdisciplinary Perspectives*. Information Science Reference, 2010, 132–161.
8. Greitzer, F.L., Purl, J., Becker, D.E. (Sunny), Sticha, P.J. and Leong, Y.M. Modeling expert judgments of insider threat using ontology structure: Effects of individual indicator threat value and class membership. In *Proceedings of the 52nd Hawaii Intern. Conf. System Sciences* (Maui, HI, USA, 2019), 3202–3211.
9. Greitzer, F.L., Purl, J., Leong, Y.M. and Sticha, P.J. Positioning your organization to respond to insider threats. *IEEE Engineering Management Review* 47, 2 (Jun. 2019), 75–83.
10. Harrison, A., Summers, J. and Mennecke, B. The effects of the dark triad on unethical behavior. *J. Business Ethics* 153, 1 (Nov. 2018), 53–77.
11. Jones, D.N. and Paulhus, D.L. Introducing the short dark triad (SD3): A brief measure of dark personality traits. *Assessment* 21, 1 (2014), 28–41.
12. Kiser, A.I.T., Porter, T. and Vequist, D. Employee monitoring and ethics: Can they co-exist? *Intern. J. Digital Literacy and Digital Competence* 1, 4 (Oct. 2010), 30–45.
13. Liang, N., Biros, D.P. and Luse, A. An Empirical Validation of Malicious Insider Characteristics. *J. Management Information Systems* 33, 2 (Apr. 2016), 361–392.
14. Montealegre, R. and Cascio, W.F. Technology-driven changes in work and employment. *Commun. ACM* 60, 12 (Nov. 2017), 60–67.
15. Paulhus, D.L. and Williams, K.M. The dark triad of personality: Narcissism, Machiavellianism, and psychopathy. *J. Research in personality* 36, 6 (2002), 556–563.
16. Sanders, G.L., Upadhyaya, S. and Wang, X. Inside the Insider. *IEEE Engineering Management Review* 47, 2 (Jun. 2019), 84–91.
17. Schultz, E.E. A Framework for understanding and predicting insider attacks. *Computers & Security* 21, 6 (2002), 526–531.
18. Shaw, E. and Sellers, L. Application of the critical-path method to evaluate insider risks. *Internal Security and Counterintelligence* 59, 2 (2015), 1–8.
19. Shaw, E.D., Post, J.M. and Ruby, K.G. Inside the mind of the insider. *Security Management* 43, 12 (Dec. 1999), 34–44.
20. Software Engineering Institute. The CERT Insider Threat Center. *Common Sense Guide to Mitigating Insider Threats, Fifth Edition*. Technical Report #CMU/SEI-2015-TR-010. SEI, Carnegie Mellon University.
21. Torres, N. It's better to avoid a toxic employee than hire a superstar. *Harvard Business Review*, 2016.
22. Veselka, L., Schermer, J.A. and Vernon, P.A. The dark triad and an expanded framework of personality. *Personality and Individual Differences* 53, 4 (Sep. 2012), 417–425.
23. Wilder, D.U.M. The psychology of espionage and leaking in the digital age. *Studies in Intelligence* 61, 2 (2017), 1–36.
24. Willison, R. and Warkentin, M. 2013. Beyond deterrence: An expanded view of employee computer abuse. *MIS Q.* 37, 1 (2013), 1–20.
25. Wu, J. and Lebreton, J.M. Reconsidering the dispositional basis of counterproductive work behavior: The role of aberrant personality. *Personnel Psychology* 64, 3 (Sep. 2011), 593–626.

Michele Maasberg (michele.maasberg@jhuapl.edu) is a Cyber Security Scientist at the Johns Hopkins University Applied Physics Laboratory, Laurel, MD, USA; <https://orcid.org/0000-0003-4306-0559>.

Craig Van Slyke (vanslyke@latech.edu) is the Mike McCallister Eminent Scholar Chair in Information Systems at Louisiana Tech University, Ruston, LA, USA; <https://orcid.org/0000-0003-3924-1859>.

Selwyn Ellis (ellis@latech.edu) is Balsley-Whitmore Endowed Professor, an associate professor, department head, and Interim Associate Dean of Graduate Programs at Louisiana Tech University, Ruston, LA, USA; <https://orcid.org/0000-0002-2816-8441>.

Nicole Beebe (nicole.beebe@utsa.edu) is Department Chair of Information Systems and Cyber Security and Melvin Lachman Distinguished Professor in Entrepreneurship Director of the Cyber Center for Security and Analytics at the University of Texas at San Antonio, TX, USA; <https://orcid.org/0000-0002-0151-1617>.