MANUSCRIPT ID NUMBER EMR-25-0163.R2

When an Insider Threat is No Longer an Insider Threat: A Look at Risk Decay

Frank L. Greitzer, PhD, Chief Behavioral Scientist, Cogility Software

***Index Terms*—information security, insider risk, insider threat, potential risk indicator.**

***Abstract*— In the realm of insider threat management, the Whole Person methodology leverages behavioral and technical indicators to identify potential risks posed by employees before they manifest into harmful actions. This article considers the concept of risk decay, which refers to the attenuation of the value or weight of potential risk indicators over time. Insider risk indicators decay rates—the timespans over which an insider risk analyst will continue to take account of an observed indicator—vary depending on the nature of the indicators. Many technical indicators that reflect transient concerns, such as login errors, have relatively short timespans of influence. In contrast, indicators that reflect more stable characteristics, such as personality traits, will be considered for much longer timespans. By examining the varying decay rates of different indicators, the article highlights the importance of incorporating decay parameters into threat assessments. The findings underscore the need for a nuanced approach to insider threat management, advocating for a deeper exploration of decay characteristics to enhance the accuracy and effectiveness of security measures.**

I. INTRODUCTION

It seems like every couple of weeks we're treated to some disturbing new story in the press about an institution being rocked by the actions of a rogue employee: a once-trusted insider who then collaborates with foreign spies, or intentionally/unintentionally leaks secrets to unauthorized sources, or perpetrates shocking acts of workplace violence (e.g., [1], [2]). Such insider threats have huge organizational impacts: Industry surveys such as the *2024 Insider Threat Report* by Cybersecurity Insiders [1] found that a staggering 83% of organizations experienced at least one insider incident in 2024, and nearly half of the organizations polled reported that insider attacks had become more frequent in the past year. The Poneman *Insider Risk Global Report* [2] notes that the average annual cost of dealing with insider risk has risen to over $17M USD, with an average of 81 days required to respond to insider incidents.

Most assessments of insider risk stress the importance of the human element: for example, the 2024 Verizon Data Breach Investigations Report found that more than two-thirds of all data breaches reflect misuse/abuse of privilege, social engineering compromises, and human errors [3]. Thus, it is imperative that organizations planning to set up or improve existing Insider Risk Management (IRM) programs incorporate behavioral factors as well as more traditional technical risk indicators into their risk assessment processes [4]. This Whole Person approach uses social, behavioral and technological indicators to identify problematic employees *before they do something harmful* [5][6]. A more proactive approach is also essential to help the IRM team identify unknown insider risks, which, by definition, may lack a pre-identified threat vector or target but where identification of relevant PRIs can still inform appropriate mitigation strategies.

The challenge, though, is that potential risk indicators (PRIs) are themselves very complex things.

Rather than being generic and interchangeable, each indicator has a certain weight or value that, when determined, can give a security analyst an idea of whether an employee might become an insider threat—and even what sort of insider threat [7]. So, for example, signs of disgruntlement (say, in social media posts or performance reviews) indicate a greater potential for future data theft or sabotage, but they don't suggest a greater likelihood of becoming a phishing victim.

What's more, these indicator values—as useful as they are—are not fixed in stone. In fact, the risk values can be reduced through protective factors, i.e., active intervention by the organization getting "left of harm" by helping a troubled individual find an offramp from the critical pathway [8]. This positive intervention might, for example, take the form of the institution providing financial counseling and other resources to debt-burdened employees, thus helping reduce the potential temptation to do something illegal.

Another way the risk values of social, behavioral and technological indicators can change is simply through *decay,* due to the passage of time. This occurs when, at some point after the first reporting of a risk indicator, the analyst may no longer consider it relevant to insider risk assessment.

The concept of decay is useful to a Whole Person approach to countering insider threats, but until recently, the phenomenon has been given short shrift in the professional literature [9][10]. So, to fill in the gaps, let's begin a foray into the topic of PRI decay and its implications for insider risk management.

II. INSIDER RISK INDICATOR DECAY

Whether it's an almost-ripe banana going black after a week out on the kitchen counter or the way our Wi-Fi signal gets

Submitted July 25, 2025. Revised October 27, 2025. Revised December 29, 2025. *(Corresponding author: Frank L. Greitzer)*

The author is with Cogility Software and PsyberAnalytix. (e-mail: fgreitzer@Cogility.com)

weaker the farther we move our wireless device from the home router, decay (biological and technical) is a familiar concept to most people. In a similar vein, the value or weight of a potential risk indicator can attenuate over time (even without the organization's leadership playing an active mitigation role).

The rate of decay varies across indicators, however. This is because different indicators are judged by expert analysts to have different decay rates.

To illustrate, let's take the case of Bob, who just returned to work from a vacation—right after his organization required everyone to change their passwords. Bob might experience several failed computer logins, which would normally generate a technical risk indicator. But after a couple months of successful logins, these authentication failures would not be considered problematic. So, this is a case of a relatively high decay rate of a potential risk indicator.

By contrast, Arnold has repeatedly ended up in meetings with HR because of his high-handed and abusive behavior towards co-workers. An analyst would likely judge Arnold to have a character flaw or personal trait that's not expected to change much over time [11]. In such a case, the potential risk indicator would have a very slow decay rate.

A. Research on PRI Decay and Related Concepts

While intuitively appealing, these examples do not provide empirical evidence for the insider risk indicator decay phenomenon. Such evidence has been reported in studies using various methods to obtain expert analyst judgments of the rate of change of insider risk over time. A survey of cyber- and insider threat professionals that obtained judgments of insider risk for scenarios with PRIs occurring at different points on a timeline found varying rates of decay for different types of PRIs [4]. In that survey study, 25 expert respondents were asked to provide level-of-concern ratings for 26 hypothetical cases based on data that spanned four months. This enabled calculation of possible PRI decay over the four-month time interval. Different types of PRIs were studied, including personal predispositions (e.g., personality factor like big ego), precipitating events (e.g., passed over for promotion), behavioral precursor (e.g., disgruntled), and technical precursor (e.g., unusual file deletion). In general, PRIs associated with personal predispositions showed very little decay compared to the other types of indicators and the likelihood that a PRI risk value exhibited a nonzero decay over time was significantly lower for personal predispositions

However, there are exceptions that lead us to reject a general rule of this nature. Another study elicited expert judgments of the time periods over which individual PRIs would be considered relevant to an insider threat analyst. In this study of expert analysts within an operational insider threat hub [10], twelve analysts rated decay rates for 265 PRIs from the Sociotechnical and Organizational Factors for Insider Threat (SOFIT) taxonomy [7]. Responses were required for each PRI, with six decay-rate response options ranging from "Very High" (dissipating 100% in 30 days) to "Very Low" (dissipating 100% in 5 years) to "None." The results revealed that:

- Analysts tend to be reluctant to assign any PRI to the highest decay rate category. Because of this finding, our update of the original SOFIT [7] taxonomy of insider threat PRIs defines three levels of PRI decay: none, low, and moderate.
- Personal predispositions like psychopathy and narcissism have little or no decay, but so does the technical precursor, Introduction of Malicious Code. Egregious cyber acts are not soon forgiven, unlike lesser cyber events like Printing to Anomalous Location.
- Some behavioral precursors (e.g., Associating with Extremist Groups) have low or no decay, but others (e.g., Attendance Issues) have moderate decay.

The preliminary estimates of these gradual PRI decay rates suggested in these studies align with related research on the longevity of grudges, which informs us that grudge-holders who are upset about a particular incident (for example, feeling that a company cheated them in some way) can remain bitter about it for decades [12]. Also, feelings of betrayal—a key predictor of the desire for revenge—decay nonlinearly over time [13][14].

B. Modeling PRI Decay

Here we consider modeling approaches for insider risk assessment that describe the PRI decay phenomenon. Several forms of decay may be considered (see Fig. 1): The simplest type of model is a *linear* decay that starts at an initial risk value and decreases linearly to zero. Another straightforward concept is modeled by a *step function* that assumes the PRI weight is constant for a time interval, after which it becomes zero. A more realistic, practical, and very common decay mechanism is an *exponential decay function* that describes phenomena that decay nonlinearly. Because the research findings described above tend to refute both a linear decay model and a step function, we have adopted an exponential decay model.

In exponential decay, the amount of decrease in a variable over a given time increment is proportional to the original value of the variable, as determined by a decay constant α. If we designate p_{ij} as the probability or weight of Indicator *i*, that is associated with a given insider threat behavior j, then we define an exponential decay function based on the time t_0 that the indicator was observed and current time t_1 (measured in days):

$$p_{ij}(t_1) = p_{ij}(t_0)\,(1-\alpha)^{(t_1 - t_0)}$$

For a variable that decays exponentially, we can calculate its *half-life* [number of days it takes to decrease to half of its original amount = $\ln(0.5)/\ln(1-\alpha)$], and we can specify the time when the value becomes negligibly small. When $\alpha = 0$, there is no decay. A moderate decay rate with $\alpha = 0.012$ yields a half-life of about two months and a one-year timespan at which the indicator weight becomes negligible. A relatively slow decay rate of $\alpha = 0.004$ produces a half-life of about six months and a timespan of about 3 years for the indicator weight to become negligible.

This article has been accepted for publication in IEEE Engineering Management Review. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/EMR.2026.3661857

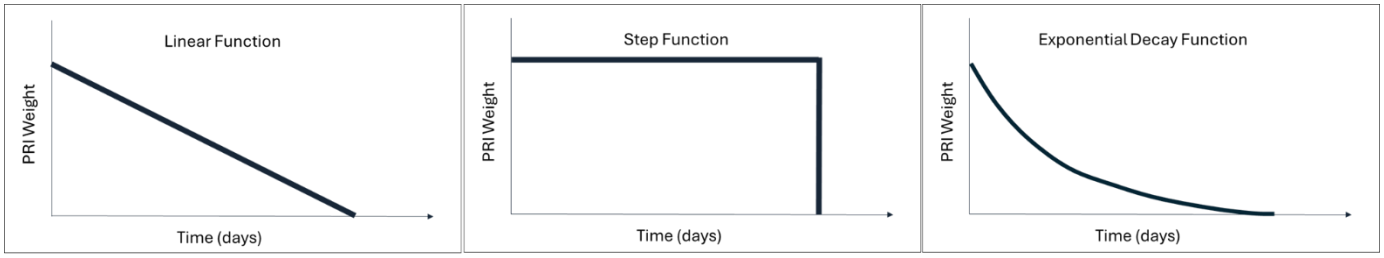

Figure 1. Examples of decay functions

In the previously-described studies with expert judgments of potential risk indicator decay rates, it was observed that analysts were reluctant to assign very high decay rates (e.g., half-life = 1 week)—even for technical indicators [10]. This may reflect a desire to avoid overlooking issues of concern. More than half of the technical indicators were assigned a decay rate with a half-life of one or two months, but 9% were considered to not decay at all. By contrast, 69% of personal predispositions were assigned zero decay rates. While these findings confirm the hypothesis that indicators have varying decay rates, additional research is needed to fine-tune these parameters. At present, the Cogynt model [15] with the SOFIT taxonomy as an underlying PRI framework uses the exponential model with three decay levels (none, $\alpha = 0$; slow, $\alpha = 0.004$; moderate, $\alpha = 0.012$). The SOFIT taxonomy is organized by PRI classes and sub-classes, with individual PRIs occupying the third/bottom level of the hierarchy. All PRIs within a sub-class have the same decay rates. A current list of SOFIT sub-classes and associated decay rates is provided in the Appendix.

III. DISCUSSION

Insider risk impacts all types of companies—small, medium, and large—across all business sectors. The most mature IRM programs use a whole-person approach with risk scoring and predictive analytics to assess potential insider threats before an incident occurs, but only 12% of organizations use well-established predictive insider risk assessment models [1]. Predictive models use estimates of PRI weights or strength of association with insider risks, often calibrated in expert knowledge elicitation studies that inform quantitative models [7]. Models help to achieve greater accuracy and consistency of outputs and to overcome the overwhelming cognitive demands on IRM analysts who must monitor, track, and assess the risk of hundreds – for large companies, even hundreds of thousands – of users. Predictive models are critically important, but incorporation of PRI decay into these models will achieve risk assessments that even more closely align with expert judgments.

A. Research Implications

This article argues that indicator decay is a worthwhile topic of discussion for organizations seeking to implement or enhance their Whole Person IRM programs. And yet, our understanding of the subject is still in its early stages—subject to limitations of initial expert knowledge elicitation studies to inform preliminary specification of decay parameters. A deeper exploration of this topic is needed to further advance the models. Research topics include:

- Additional expert knowledge elicitation studies to validate the proposed exponential decay function and its three levels of decay.
- An examination of the dynamic effects of PRIs that occur after an initial occurrence of the same or different indicator(s) that may have undergone some decay.
- Furter study of the impact of *protective factors*, which represent a different type of dynamic that diminishes the impact of PRIs.

B. Managerial Implications

As important as risk indicator decay is for fine-tuning insider threat calculations, estimating various rates of decay can be a very labor-intensive process. Thus, an organization might be tempted to defer consideration of PRI decay and treat all indicators as static over time. This is especially true for counter-insider threat programs with very limited resources. To the IRM manager who is tempted to err on the side of caution and treat PRIs as static constructs even though evidence suggests otherwise, consider this: While treating risk factors as static serves a conservative, overly cautious approach that avoids being blamed for letting a bad actor slip through cracks, there's a clear downside: First, you increase the chance of false positives that waste resources while you chase phantom threats. Second, it can lead to rather expensive wild goose chases by an organization's security analysts. Third, you also run the risk of alienating employees who have been erroneously targeted, producing aggrieved employees who might seek revenge in the future—thus creating the very outcome you seek to eliminate.

IV. CONTRIBUTION

This paper provides engineering managers with actionable insights for improving insider risk management programs. By describing the concept of risk decay, it demonstrates how the relevance of technical, behavioral, and psychological risk factors changes over time. The paper offers a practical framework for categorizing and modeling PRI decay, enabling managers to prioritize resources more effectively and reduce false positives that can waste time and erode employee trust. Incorporating decay rates into risk assessment models helps analysts make more informed decisions, balancing security needs with operational efficiency. The paper also highlights areas for future research, including studies aimed at refining PRI decay

parameters and integrating protective factors into risk assessment models. It is hoped that this article will encourage and support IRM managers in building more adaptive and cost-effective personnel and enterprise security strategies.

REFERENCES

[1] Cybersecurity Insiders. (2024). *2024 Insider Threat Report: Trends, challenges, and solutions*. https://go1.gurucul.com/2024-insider-threat-report

[2] Poneman Institute. 2025. *Cost of Insider Risks Global Report 2025*. Poneman / DTEX. https://www2.dtexsystems.com/l/464342/2025-02-19/583csx/464342/1740000012hNhGjMpn/2025_Cost_of_Insider_Risks_Global_Report_by_Ponemon_and_DTEX.pdf?_gl=1*1b5ol6j*_gcl_aw*R0NMLjE3NDk0MTk4OTIuRUFJYUlRb2JDaE1JdU0tYjktamlqUU1WR2p4RUNCMUI1UVZfRUFBWUFTQUFFZ0pnblBEX0J3RQ..*_gcl_au*MjY4NzI5MjgwLjE3NDk0MTk4OTI.

[3] Verizon. 2024. 2024 Data Breach Investigations Report. https://www.verizon.com/business/resources/Tb2/infographics/2024-dbir-finance-snapshot.pdf

[4] F.L. Greitzer, J. Purl, Y. M. Leong, and P. J. Sticha. 2019. Positioning your organization to respond to insider threats. *IEEE Engineering Management Review, 47(2)*, 75-83. https://ieeexplore.ieee.org/document/8704879

[5] D. Cappelli, A. Moore and R. Trzeciak. 2012. *The CERT Guide to Insider Threats*. New York: Addison-Wesley.

[6] F. L. Greitzer. 2019. Insider Threat: It's the HUMAN, Stupid! In *Proceedings of the Northwest Cybersecurity Symposium*, April 8-10, 2019. Article No. 4, pgs 1-8. ACM ISBN 978-1-4503-6614-4/19/04. https://doi.org/10.1145/3332448.3332458

[7] F. L. Greitzer, J. Purl, Y. M. Leong and D. E. Becker. 2018. SOFIT: Sociotechnical and Organizational Factors for Insider Threat. IEEE Security and Privacy Workshops (SPW), Workshop on Research for Insider Threat (WRIT), San Francisco, CA, May 24, 2018, pp. 197-206. DOI: 10.1109/SPW.2018.00035

[8] E. Shaw, and L. Sellers, "Application of the critical-path method to evaluate insider risks." *Studies in Intelligence, 2015, 59(2)*, 41-48.

[9] F. L. Greitzer and J. Purl, "The dynamic nature of insider threat indicators." *Springer Nature Computer Science*, 2022, 3(102).

[10] F. L. Greitzer, R. A. Kliner, and S. Chan, S. "Temporal effects of contributing factors in insider risk assessment: Insider threat indicator decay characteristics", in *Proc. of WRIT Workshop*, Austin, TX, December 5, 2022.

[11] D. A. Cobb-Clark and S. Schurer, "The stability of big-five personality traits." *Economics Letters*, 2012, *115(1),* 11-15.

[12] H. K. Hunt, H. D. Hunt, and T. C. Hunt, "Consumer grudge holding." *Journal of Customer Satisfaction, Dissatisfaction, and Complaining Behavior*, 1988, *1*, 116-118

[13] Y. Gregoire, T. M. Tripp, and R. Legoux, "When customer love turns into lasting hate: The effects of relationship strength and time on customer revenge and avoidance," *Journal of Marketing,* 2009, *73(6), 18-32*

[14] T. M. Tripp and Y. Gregoire, "When unhappy customers strike back on the Internet." *MIT Sloan Management Review, Reprint 52303, 2011, pp.1-8.*

[15] F. L. Greitzer. (submitted for publication). From patterns to predictions: Insider risk modeling with a pattern-based behavioral analytic model.

APPENDIX

Shown in Table 1 is a list of SOFIT taxonomy classes (100-level ID numbers) and sub-classes (10- or 20-level IDs), with labels, descriptions provided and associated decay rates that apply to all PRIs within a given sub-class. This material reflects the updated SOFIT2.0 taxonomy. PRI "weights" or risk values are not shown. Users of the taxonomy and/or the Cogynt insider risk model based on SOFIT generally begin with these associated parameters but may revise the assigned values based on individual organizational priorities and preferences. The complete SOFIT2.0 taxonomy listing individual PRIs is available at https://cogility.com/sofit2/.

Table 1. PRI Decay Rates Associated With SOFIT Sub-Classes

ID #	Class/Sub-Class Label	Description	Decay Rate (α)
100	Boundary Violations	Action by a person that is outside of normal or accepted behaviors. This may include actions up to the level of organizational policy violations.	
120	Concerning Work Habits	Work habits and patterns that are potentially of concern for an enterprise. Example: Working at unusual hours	Moderate (0.012)
140	Policy Violations	Minor violation of organization's security policies. Example: Tailgating	Moderate (0.012)
160	Compliance Violations	Individual has not complied with organizational requirements. Example: Expense violation	Slow (0.004)
200	Security Violation	Breaches of security regulations, procedures, guidelines etc.	
220	Minor Security Violations	Minor security violation. Example: Losing one's security badge.	Slow (0.004)
240	Major Security Violations	Copying, Disclosure, Mishandling of classified information etc. Example: Improper discussion of classified material	Slow (0.004)

280	Weapon Possession Issues	Possession or unauthorized use of a weapon Example: Illegal use of a weapon	Slow (0.004)
300	Job Performance	Negative job feedback	
320	HR Concerns	Negative performance report, etc. Example: Poor performance	Moderate (0.012)
340	Nonjudicial Punishment	Received reprimand, discipline, sanctions Example: Person has been suspended.	Slow (0.004)
360	Concerning Job Status	Employment status (e.g., new hire, retiring, resigned, terminated). Example: Resigned to take another job.	Moderate (0.012)
400	Financial Concern		
420	Unexplained Affluence	Observed change in means (financial status) where no logical income source exists. Example: Living beyond one's means	Slow (0.004)
440	Credit and Debt Concerns	Credit or debt concerns. Example: Credit problems	Slow (0.004)
500	Foreign Ties		
520	Foreign Affiliations	Foreign affiliations. Example: Active foreign passport	No Decay (0)
540	Foreign Contacts	Foreign contacts. Example: Unreported contact with foreign national	Slow (0.004)
560	Foreign Travel	Suspicious foreign travel. Example: Change pattern of foreign travel	Slow (0.004)
580	Foreign Assets	Possession of foreign assets. Example: Foreign business or political interests	Slow (0.004)
600	Criminal Activities	A person's Criminal Record	
620	Criminal Record involving Violence	Criminal record involving violence: Example: Domestic violence	No Decay (0)
640	Other Criminal Acts or Records	Other criminal records Example: financial crime (fraud, theft)	Slow (0.004)
700	Ideology	A person's set of beliefs that are publicly expressed, with possible intent to influence the orientation or actions of others.	
720	Affiliations	Identification or affiliation with a group that is associated with activities aimed at harming the organization. Example: Associating with extremist or terrorist group	No Decay (0)
740	Beliefs	Expressions of ideology that legitimize terrorism/violence Example: Communicating radical beliefs	No Decay (0)
800	Psychosocial Factors	Psychological factors	
820	Behavioral Health Issues	Behavioral or psychological problems of sufficient severity and/or duration to cause markedly impaired functioning and/or marked distress. Example: Substance abuse	No Decay (0)
840	Interpersonal Issues	Interpersonal issues. Example: Aggression	Slow (0.004)
850	Personal Stressors	Personal stressors. Example: Relationship break-up	Slow (0.004)
860	Discontent	Expressions discontent. Example: Disgruntlement	Slow (0.004)
880	Personality or Character Traits	A person's personality traits Example: Low-conscientiousness	No Decay (0)
900	Cybersecurity Violation	Action on workstation or organization's network that may introduce or increase vulnerability to cyber attack.	
910	Endpoint with Active Compromise	Computing resource whose confidentiality, integrity or availability has been adversely impacted. Example: Use of unapproved software	Slow (0.004)
920	Authentication Authorization	Attempt to defeat network authentication/authorization for access to sensitive material. Example: Failed login attempts	Moderate (0.012)

930	Data Access Anomalies	Attempt to access sensitive data or data that is beyond user's privilege and/or scope of work. Example: Attempt Unauthorized Access to Sensitive Data	Moderate (0.012)
940	Network Patterns	Unauthorized or suspicious actions on network. Example: Violating web policy	Moderate (0.012)
950	Cyber Obfuscation	Concealing activities on workstation or network. Use of covert channels	No Decay (0)
960	Data Transfer Patterns	Suspicious means of transferring data. Example: Excessive printing of documents	Slow (0.004)
970	Command Usage	Use of operating system commands to gain control of, attack, or compromise a computer system. Example: Disabling security features	No Decay (0)
980	Data Manipulation	Unauthorized modification or destruction of data. Example: Delete or edit audit logs	No Decay (0)
990	Suspicious Communication	Suspicious communication pattern. Example: Suspicious communication with foreign entities	Slow (0.004)

Frank L. Greitzer, PhD received a B.S. degree in Mathematics from Harvey Mudd College, Claremont CA USA, a M.A. degree in Psychology and Ph.D. in Mathematical Psychology from UCLA, Los Angeles CA USA. He serves as the Chief Behavioral Scientist at Cogility Software and is the founder and Principal Scientist at PsyberAnalytix. Prior to founding PsyberAnalytix in 2012, he worked as a research psychologist for the US Navy, a human factors and AI researcher in the aerospace industry, and Chief Scientist in cognitive informatics at the U.S. DOE Pacific Northwest National Laboratory. At Cogility, he supports development and deployment of advanced decision intelligence solutions including insider risk management. Dr. Greitzer's contributions to research and practice include numerous journal articles, conference papers, and invited talks.

Byline:
Frank L. Greitzer PhD, Chief Behavioral Scientist, Cogility Software