Insider Threat Indicator Decay

COGILITY

Contents

Introduction and Background 1
Deeper Dive into Possible PRI Decay Models 3
Analysis of Role Types and PRI Decay 3
PRI Severity 5
PRI Intent Ambiguity 6
Discussion and Limitations 9
Summary 9
Limitations 10
Proposed Empirical Study 11
Empirical Study of Role Type and Severity Factors 11
Empirical Study Incorporating the PRI Intent Ambiguity Factor 12
A Three-Factor Study Design 13
Conclusions and Recommendations 14
References 15

List of Figures

Figure 1. PRI Decay Rate Judgments by Role Type and PRI Severity 5
Figure 2. Relationship Between Judgments of Decay Rate and PRI Intent Ambiguity 9
Figure 3. Relationship Between PRI Decay Rate, Role Type, and Intent Ambiguity 10
Figure 4. Sample question about PRI decay rate 12

List of Tables

Table 1. Distribution of Decay Rates Across Role Types 4
(a) Distribution across four decay rate levels 4
(b) Distribution across two decay rate levels (Combining HIGH/MEDIUM and LOW/NO Decay) 4
Table 2. Number of Low vs. High Severity PRIs by Decay Rate 6
Table 3. Representative Sample of PRIs Indicating Associated Decay Rate and Intent Ambiguity 8
Table 4. PRI Selections for two-Factor Study of Role Type and Severity 11
Table 5. PRI Selections for two-Factor Study of Role Type and Intent Ambiguity 13
Table 6. PRI Selections for Three-Factor Study of Role Type, PRI Severity, and PRI Intent Ambiguity 14

Introduction and Background

Indicator decay refers to the possible decline in the impact of an insider threat Potential Risk Indicator (PRI) over time. This refers to the "influence" of an observed insider threat indicator on the Analyst's judgment of insider risk, as a function of time. Earlier research [1] provided evidence that insider threat indicators may have varying temporal effects on judgments of insider risk and that some PRIs (such as those representing personal predispositions) are more likely to have a persistent impact – i.e., exhibiting little or no decay—than other types of PRIs (such as behavioral or technical precursors that have a decreasing impact on risk judgments over time. Subsequent research described a preliminary model for PRI decay [2] and conducted an expert knowledge elicitation study to test the model [3] using a large set of PRIs. Results suggested that there are systematic differences in PRI "half-life" based on indicator characteristics. To serve as background for the present extension of this work, we provide a brief overview of the findings reported in [3].

To study decay characteristics of PRIs, we merged the indicators defined in a comprehensive insider threat indicator ontology (Sociotechnical and Organizational Factors for Insider Threat, SOFIT) [4] and a DoD taxonomy, producing a set of ~265 PRIs. We followed [1] in categorizing the PRIs along the dimension referred to as "Role Type" since preliminary indications are that PRIs might differ in their decay parameters based on Role Type. Four main categories of Role Type are:

- ***Precipitating Event.*** An event that triggers or motivates the insider to carry out an insider crime. [Examples: *disciplinary action, passed over for promotion, revocation of security clearance*]
- ***Personal Predisposition.*** A (personal) characteristic historically linked to a propensity to exhibit malicious insider behavior. [*Examples: gambling addiction, mental instability, self-harm, suicidal ideation*]
- ***Behavioral Precursor.*** An individual action, event, or condition that involves personal or interpersonal behaviors and that precedes and is associated with insider activity. [Examples: *attempts to obtain national security information without need-to-know, criminal behavior involving weapons, verbal abuse/bullying*]
- ***Technical Precursor.*** An individual action, event, or condition that involves computer or electronic media and that precedes and is associated with malicious insider activity. [Examples: *disabling anti-virus software, excessive use of screen capture, sending E-mail to suspicious address*]

As described in [3] of this report, a knowledge elicitation survey was conducted with twelve experts at the DoD/Department of the Air Force (DAF) insider threat hub in San Antonio, Texas.

The experts were briefed on decay and associated "half-life" characteristics and then provided judgments of the rate of decay for each PRI, using a six-point scale:

- Very High – impact dissipates to zero in one month; half-life = 1 week
- High – impact dissipates to zero in six months; half-life = 1 month
- Medium – impact dissipates to zero in one year; half-life = 2 months
- Low – impact dissipates to zero in three years; half-life = 6 months
- Very Low – impact dissipates to zero in five years; half-life = 1 year
- No-Decay/None – impact does not decrease over time

The interrater reliability was only "fair to moderate" in this study but the analysis indicated a highly significant association between Role Type and the six decay rate levels. To illustrate the most reliable effects in this study, we converted the six-level decay-rate scale into a four-level scale by combining some of the decay-rate categories— Very High and High categories were combined and denoted HIGH; MEDIUM was unchanged; Low and Very Low categories were combined and denoted LOW; and NO-DECAY was unchanged; we then focused on the set of PRIs that were most consistently assigned (by at least six of the twelve experts) to one of the four decay rate categories. The following trends were observed:

- Technical Precursors are much less likely to be assigned a no-decay rating (only 9% of these indicators were rated in the no-decay category). Over one-half (56%) of the Technical Precursors were assigned Medium to Very High decay rates.
- Personal Predispositions, in contrast, were most likely to receive no-decay or low decay rate estimates (69%). They were least likely to be identified with high or very high rates of decay (11%).
- Behavioral Precursors were very likely to be considered to have no-decay or low decay rates (70%). Forty-one percent of the Behavioral Precursors were assigned to the Medium-to-Very High decay rate categories.
- Precipitating Events were very unlikely to be assigned a no-decay rating (6%) but were relatively likely to be considered to have very low to medium decay rates (70%).

We also observed that our expert analysts seemed reluctant to assign the Very High decay rate category to PRIs—only 4% of Behavioral Precursors and Personal Predispositions were assigned the Very High decay rate; 6% of Precipitating Events were assigned the Very High decay rate; and 8% of Technical Precursors were assigned this rate of decay. This may reflect the fact that the analysts wish to avoid overlooking issues of concern.

In summary, these findings confirm the general observation that insider threat indicators decay at different rates, with some distinctive differences based on indicator Role Types. Since it appears that there are also variations within Role Types, the article recommended that the Role Type classes could be broken down into two or three subclasses for purposes of assigning decay rates.

Deeper Dive into Possible PRI Decay Models

Since publication of the results in [3], additional analyses of the data obtained in the PRI decay judgment study have led to new insights. First, we examine the Role-Type factors more closely; then we consider more complex PRI decay models.

Analysis of Role Types and PRI Decay

In this analysis, we continued to use the modified four level decay rate scale (HIGH, MEDIUM, LOW, NO-DECAY) and focused on PRIs that were most consistently assigned to these four decay rate categories (receiving at least six of twelve decay rate assignments in the same decay rate category). Since there were twelve expert participants in the study, it was possible that ties can occur (e.g., six ratings in two different decay rate categories). In fact, this occurred for nine of the 265 PRIs: in six of these cases, the PRIs were in the Behavioral Precursor role type and the ties occurred for the LOW and the NO-DECAY categories.[1] For these cases, we adopted the most conservative approach to assign the PRIs to the NO-DECAY category. Three other ties occurred for PRIs in the Technical Precursor role type. One PRI (Encrypted protocols) had six MEDIUM decay ratings and six LOW decay ratings—it was assigned to the LOW decay category. Two PRIs (Excessive printing or fax and Significant change in Internet activity) had six assignments in HIGH decay and six in MEDIUM decay categories; again, we adopted the conservative approach that assigned these PRIs to the MEDIUM decay category for purposes of this analysis. Of the 265 PRIs, 83 PRIs did not exceed the criterion for a minimum of six judges agreeing on a rating – these were excluded from the analysis. This still left a total of 182 PRIs to analyze: 9 of 13 Precipitating Events, 11 of 26 Personal Predispositions, 92 of 119 Behavioral Precursors, and 70 of 107 Technical Precursors.

The distribution of decay rates across the four Role Types is shown in Table 1a, b. Several observations are evident:

- Precipitating events are typically assigned the LOW decay rate (67%)
- Personal Predispositions are strongly associated with LOW or NO Decay rates (91% in total)
- Behavioral and Technical Precursors are distributed across the different decay rate levels.

1 The PRIs were: Communicating endorsement of workplace violence, communicating extremist views, Criminal behavior involving weapons, Criminal violent behavior including sexual assault and domestic violence, Unauthorized contact with officer/agent of a foreign intelligence agency, and Carrying classified information on foreign travel without authorization.

Table 1. Distribution of Decay Rates Across Role Types
(a) Distribution across four decay rate levels

Role Type	HIGH Decay	MEDIUM Decay	LOW Decay	NO Decay	Total
Precipitating Events	2 (22%)	1 (11%)	6 (67%)	0 (0%)	9
Personal Predispositions	0 (0%)	1 (9%)	5 (45%)	5 (45%)	11
Behavioral Precursors	9 (10%)	20 (22%)	48 (52%)	15 (16%)	92
Technical Precursors	11 (15%)	23 (32%)	35 (49%)	1 (1%)	71

(b) Distribution across two decay rate levels (Combining HIGH/MEDIUM and LOW/NO Decay)

Role Type	HIGH / MEDIUM	LOW / NO DECAY
Precipitating Events	33%	67%
Personal Predispositions	9%	91%
Behavioral Precursors	32%	68%
Technical Precursors	49%	51%

An expedient conclusion from these findings is that two of the four Role Types – Precipitating Events and Personal Predispositions – are strongly associated with specific PRI decay rates:

- Precipitating Events may be expediently considered to exhibit the LOW rate of decay (half-life ~ 6 months; dissipates completely in ~ 3 years)
- Personal Predispositions may be expediently considered to exhibit a LOW to NO-DECAY rate of decay. A conservative assignment is to consider these to have NO DECAY. A compromise assignment is to use the original Very Low decay rate category (half-life ~ 1 year; dissipates completely in ~5 years).

It is obvious that decay rates for the other two Role Types cannot be predicted reliably using Role Type alone: A PRI decay model for Behavioral or Technical Precursors likely depends on some other factor—possible two-factor models are examined in Sections PRI Severity and PRI Intent Ambiguity.

PRI Severity

The original study [3] posited a possible relationship between PRI severity and role type in determining PRI decay rate. Figure 1, below, reproduces a portion of the results shown in Table 3 of [3], displaying a selection of PRIs with the most consistent decay rate assignments that fall into the four major decay rate levels; tentative exponential decay rate parameters are also indicated in the table.[2] Since there is a more "pure" relationship between decay rates and both Precipitating Events and Personal Predispositions, here we only examine severity scores for Behavioral Precursors and Technical Precursors. We have added average severity values (on a 0.0-1.0 scale) of these PRIs, shown in brackets.[3]

Role Type	Decay Rate Characterization			
	No Decay	Very Low/Low	Medium	High/Very High
Behavioral Precursor	• Associating with extremist or terrorist groups • Workplace violence • Advocating terrorism or violence *[0.9]*	• Delinquent debts • Substance abuse • Travel policy violation *[0.5]*	• Adverse changes to financial status • Declining performance • Security violation • Attendance issues *[0.5]*	•
Technical Precursor	• Introduction of malicious code *[0.9]*	• Unauthorized storage device • Unauthorized wireless *[0.7]*	• Large data transfers • Change file extensions • Printing to anomalous location *[0.7]*	•
Tentative/Recommended Decay rate range	$\alpha \sim 0.0$ *Half-life ~ ∞*	$0.00385 < \alpha < 0.002$ *Half-life ~ 6mos./1 year*	$\alpha \sim 0.012$ *Half-life ~ 2 months*	$0.025 < \alpha < 0.15$ *Half-life ~ 1 week*

Figure 1. PRI Decay Rate Judgments by Role Type and PRI Severity

It is evident that as the decay rates change from No Decay to High decay moving across the table from left to right, the severity scores tend to decrease: For the three Behavioral Precursor PRIs exhibiting no decay and one Technical precursor exhibiting no decay, the average severity of both behavioral and technical PRIs was 0.9; and the severity scores are lower for PRIs that were ranked in the Low or Medium categories. This suggests that PRI severity may influence the judged decay rate, in addition to role type. This conjecture was investigated using the data obtained in the decay study [3].

To see if there is a relationship between PRI decay rates and the severity scores for Behavioral and Technical Precursors, we computed percentile ranks of all PRIs, within their Role Types. Then we defined two levels of severity (low, high) where PRIs with severity percentile scores below the 80th percentile

2 In mathematical terms, it is convenient to use a general and extensively used exponential decay model $S(t) = S_0 e^{-\alpha t}$, which assumes that the amount of decay, from one time to the next, is proportional to the original value of the variable. Here, the variable S is the severity of the PRI; S_0 is the initial severity and S(t) is the severity at time t. The alpha parameter specifies the decay rate.

3 These severity scores were obtained in previous research, unrelated to the current studies.

were considered to have Low Severity, and PRIs with severity scores above the 80th percentile were considered to have High Severity. The number of Low versus High Severity PRIs falling in the four decay rate categories is shown in Table 2. A chi-square test of association shows that there is not a significant relationship between Severity and Decay rate for the PRIs within the two role types, Behavioral Precursors and Technical Precursors.

Table 2. Number of Low vs. High Severity PRIs by Decay Rate

	HIGH Decay	MEDIUM Decay	LOW Decay	NO Decay
Low Severity	2 (6%)	8 (23%)	21 (60%)	4 (11%)
High Severity	20 (14%)	37 (25%)	73 (50%)	17 (11%)

To summarize, while Role Type provides a reasonable indication of PRI decay rate for Precipitating Events and Personal Predispositions, the other role types (Behavioral, Technical Precursors) are not strongly indicative of PRI decay; and taking PRI severity into account does not help to distinguish different decay rates assigned to Behavioral and Technical Precursors.

PRI Intent Ambiguity

It is useful to examine other possible factors that may influence how long an analyst will consider the impact of a PRI after it has been observed/reported. One potentially relevant factor is the "clarity" of the intent of the PRI—a factor that we denote "Intent Ambiguity." A rationale for using a relationship between intent ambiguity and PRI decay is the sense that the more clearly the act can be interpreted as malicious, the longer it will be considered to inform the threat analysis. Consider some examples that use a simple two-level classification of Intent Ambiguity (Ambiguous Intent, Clear Intent):

- PRI: Passed over for promotion – *Ambiguous Intent.* This PRI does not provide any insight into the possible intent of an insider threat—it is ambiguous with respect to understanding intent. In the absence of any other observed PRIs, it is reasonable to expect that this PRI would not persist a long time in analyzing possible insider risk.
- PRI: Narcissism – *Ambiguous Intent*. Once again, observation of this PRI does not inform an analyst about possible motivation/intent to harm the organization. Taken alone, this PRI is ambiguous with respect to understanding possible intentions to act maliciously against the organization.
- PRI: Violence directed against people – *Clear Intent*. This PRI inherently implies malicious intent. It should be regarded as Not Ambiguous.

- PRI: Associating with extremist or terrorist groups – *Clear Intent.* An individual who associates or advocates extremist or terrorist acts should be considered to have unambiguous malicious motivation/intent.
- PRI: Attempt unauthorized access to sensitive data – *Clear Intent.* Attempted or successful unauthorized access to sensitive data reflects malicious intent.

With this construct in mind, we can examine the possible relationship between PRI risk decay judgments obtained in the original study and the intent ambiguity features of the PRIs used in that study. As noted above, the limitations due to less-than-desirable inter-rater reliability of the decay rate judgment data in the original study still apply; to help address this problem, as described above, we have confined the analysis to those PRIs for which at least six of the 12 analysts agreed on decay ratings. In addition, there has been no opportunity for an expert knowledge elicitation exercise to obtain judgments of intent ambiguity for these PRIs. Instead, as a preliminary exploration of the data, the author alone has categorized the intent ambiguity of the PRIs for this analysis.

Table 3 provides a small, representative sample of PRIs, organized by Intent Ambiguity (as judged by the author) and Decay Rate judgments obtained in the original study.[4] The values for these variables are indicated for each PRI by placing a checkmark (✓) in one of the four Decay Rate columns and a checkmark in one of the two Intent columns. For the entire set of 182 PRIs in the four role type categories, we found that all nine PRIs in the Precipitating Event Role Type are considered to have Ambiguous Intent; and nine of eleven PRIs in the Personal Predisposition Role Type are associated with Ambiguous Intent. As discussed in the previous section, a simple (one-factor Role Type) model seems sufficient to classify decay rates for these two Role Types; therefore, the consideration of Intent Ambiguity as a factor will be focused on the other two Role Types (Behavioral and Technical Precursors).

4 Representative Sample of PRIs Indicating Associated Decay Rate and Intent Ambiguity.

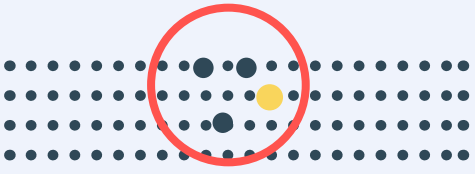

Table 3. Representative Sample of PRIs Indicating Associated Decay Rate and Intent Ambiguity

PRI	Decay Rate				Intent Ambiguity	
	No-Decay	LOW	MEDIUM	HIGH	Ambiguous Intent	Clear Intent
Demotion		✓			✓	
Pending Transfer				✓	✓	
Gambling Addiction			✓		✓	
Narcissism	✓				✓	
Psychopathy	✓				✓	
Associating with Extremist or Terrorist Groups	✓					✓
Communicating Extremist Views	✓					✓
Illegal Substance Abuse or Trafficking		✓			✓	
Enabling or Facilitating Extremist Organization	✓					✓
Obfuscate Report of Foreign Contact		✓				✓
Unauthorized Copying of Classified Info		✓				✓
Changes to Firewall Settings		✓				✓
Printing to Anomalous Location			✓		✓	
Sending Email with Large Attachments				✓	✓	
Using Unapproved Encryption Software			✓			✓
Large Data Transfer Outgoing			✓			✓

The relationships between Intent Ambiguity and Decay Rates for Behavioral and Technical Precursors are graphically depicted in Figure 2.

- For Behavioral Precursors, 69 of 92 PRIs are considered to have Ambiguous Intent, and these were predominantly judged to have Low or Medium decay rates (58 of 69 PRIs, 84%). All 23 PRIs (100%) considered to have Clear Intent were judged to have either Low or No decay.
- For Technical Precursors, 43 of 70 PRIs are considered to have Clear Intent and 30 of these (70%) were judged to have a LOW decay rate. The 27 Technical Precursors considered to have Ambiguous Intent were predominantly assigned MEDIUM or HIGH decay rates (12 to MEDIUM, 10 to HIGH, 5 to LOW).

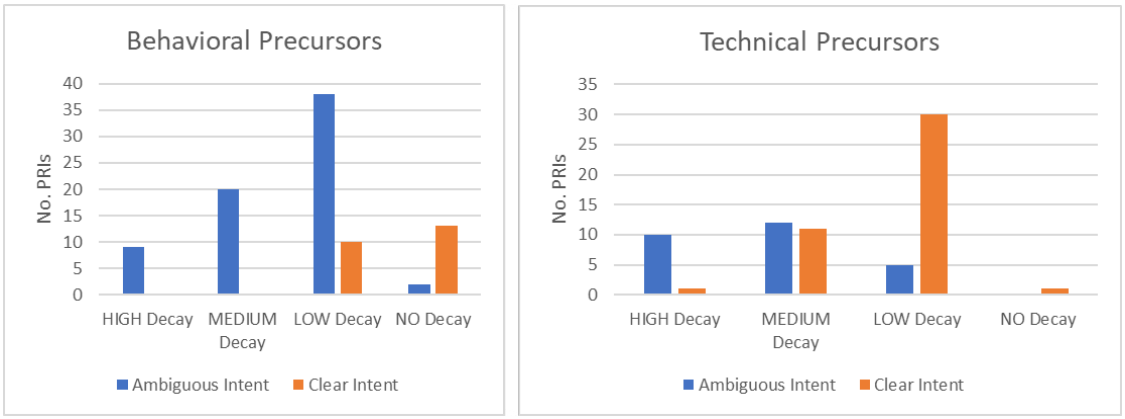

Figure 2. Relationship Between Judgments of Decay Rate and PRI Intent Ambiguity

Based on these findings, an expedient (and conservative) rule for assigning PRI decay rates to Behavioral or Technical Precursors is:

- Behavioral Precursors with Clear Intent → NO decay
- Behavioral Precursors with Ambiguous Intent → LOW Decay rate
- Technical Precursors with Clear Intent → LOW Decay rate
- Technical Precursors with Ambiguous Intent → MEDIUM Decay rate.

Discussion and Limitations

Summary

Results of the current study as well as prior research examining the relationship between PRI Role Types and PRI decay rates—using widely differing methods for extracting expert judgments--indicate that PRI decay rates are directly related to two types of PRI Role Types: Precipitating Events and Personal Predispositions. There is consistent evidence that Precipitating Events decay at a low rate and Personal Predispositions may be characterized as exhibiting no decay (or very low rate of decay). In contrast, Behavioral Precursors and Technical Precursors do not exhibit a simple/direct relationship with PRI decay rate categories.

The present examination of data obtained in [3] found no systematic relationship between PRI decay rates and PRI severity; in addition, we found no systematic relationship between decay rate and relative severity within a Role Type—no evidence for a two-factor model, despite a conjecture by [3] that decay rates might be predictable by taking both Role Type and severity into account. The present study also investigated possible relationships between a new construct, “Intent Ambiguity,” and decay rates for Behavioral and Technical Precursors.

There seemed to be a relatively consistent relationship for Behavioral Precursors, such that those PRIs that reflect ambiguous intent tend to be judged as having low decay rates, while those that reflect clear intent tend to be judged to have no decay. For Technical Precursors, those with Clear Intent tend to be characterized as having LOW decay; those with Ambiguous Intent may be characterized as having LOW or MEDIUM Decay rates., with a slight preference for MEDIUM. These relationships are depicted in Figure 3, with suggested values of α, the exponential decay rate parameter.

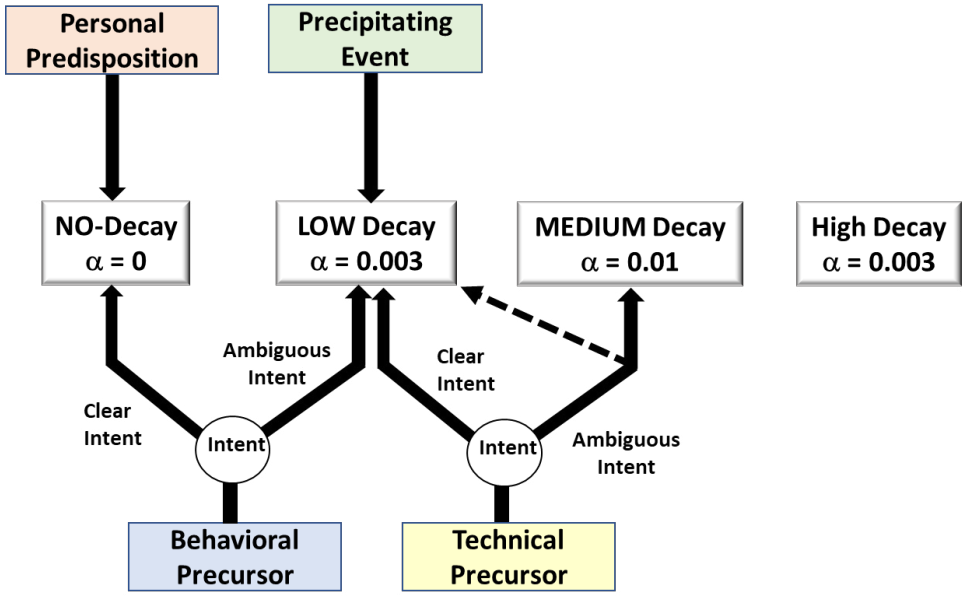

Figure 3. Relationship Between PRI Decay Rate, Role Type, and Intent Ambiguity

Limitations

There are several limitations of the analyses reported here:

(a) The less-than-desired inter-rater reliabilities found in the original PRI decay rating study adversely impact these results. Inter-rater reliability problems suggest that the decay rating task is difficult. As may be seen by reviewing the methodology described in the original study [3], one source of variability could be inadequate “preparation” of the experts: The subject-matter experts were provided only a brief explanation about PRI decay that included depiction of decay curves and “half-life” values for various rates of decay. Whether these instructions provided a useful context for the analysts is not known. A second possible contribution to inter-rater variability is the use of six decay-rate categories, which could have introduced additional complexity and difficulty. The present work sought to address this difficulty in the data analysis by combining the six decay rate categories into only four. Nevertheless, this strategy did not appreciably improve the results. Whether or not use of a simplified scale in the knowledge elicitation exercise would improve inter-rater reliability is a question that merits further study.

(b) In our assessment of the role of PRI severity (Section 2.2), we note that the severity scores came from two different sources: Severity scores for PRIs that derived from SOFIT were based on earlier research on SOFIT indicators; PRIs that came from the DAF-InT program had severity scores that were estimated by the DAF-InT program, and these severity scores have been described as preliminary. Variability in severity scores may cloud the results of this analysis.

(c) In our assessment of the role of PRI Intent Ambiguity, the ambiguity judgments came from the author of this report. A more robust examination of this construct would require further expert knowledge elicitation studies.

Proposed Empirical Study

Empirical Study of Role Type and Severity Factors

A study can be designed to distinguish separate and combined effects of Role Type and PRI severity on judgments of PRI decay. The expert knowledge elicitation task would ask our expert analysts to judge the decay rates (none, low, medium, high) of different pairs of sixteen PRIs selected from the four role type categories (see Table 4). Within each Role Type, two PRIs are representative of high severity indicators and two are representative of low severity indicators. The PRIs used in the study need not be the same for all participants—different sets of PRIs may be used to the extent that representative high-severity vs. low-severity PRIs may be identified.[5]

Table 4. PRI Selections for two-Factor Study of Role Type and Severity

Role Type	High Severity PRIs	Low Severity PRIs
Personal Predisposition	PRI-1 PRI-2	PRI-3 PRI-4
Precipitating Event	PRI-5 PRI-6	PRI-7 PRI-8
Behavioral Precursor	PRI-9 PRI-10	PRI-11 PRI-12
Technical Precursor	PRI-13 PRI-14	PRI-15 PRI-16

The expert knowledge elicitation task will ask the experts for judgments about how long each PRI will influence their insider threat assessments. This requires only 16 questions. If we wish to further generalize the set of PRIs, we may pick another set of 16 PRIs in accordance with Table 4 and then ask for another set of 16 decay rate judgments, for a total of 32 judgments.

5 At the discretion of the experimenter(s), an initial expert knowledge study may be performed to pick representative high versus low severity PRIs within each role type category. This may not be necessary if the experimenters are confident in their ability to discriminate PRIs based on severity.

For the survey used in this study, each question begins with a description of the PRI to be considered. The expert is asked to estimate the decay rate of the PRI described by indicating how long the PRI would continue to be taken into consideration. If the analyst indicates that the influence of the PRI will decrease over time, then we ask for judgments about how long the PRI would continue to have an influence (1 week, 1 month, 6 months, 1 year, 3 years, other). A sample question is shown in Figure 4.

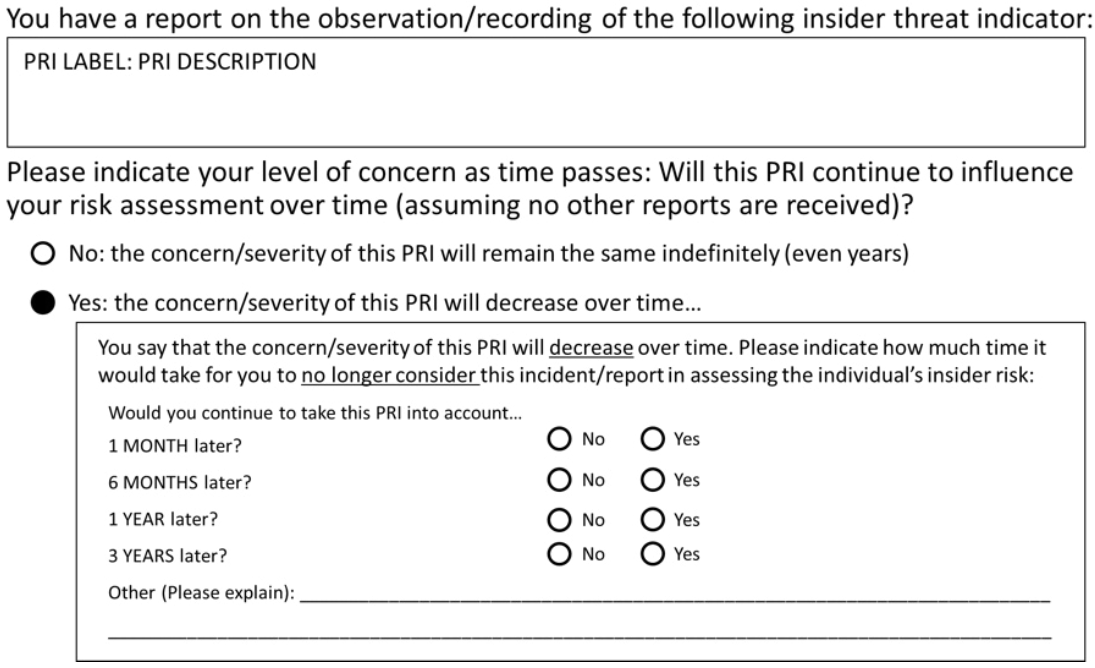

Figure 4. Sample question about PRI decay rate

The questions that are posed in the proposed new PRI decay study offer a different approach to estimating PRI decay rates, compared with the earlier study that produced lower than desired inter-rater reliabilities. The questions on PRI decay that are used in the proposed study seek estimates of "time scale of influence" by obtaining judgments about the length of time a PRI will influence the expert's threat assessment. We can use these judgments to estimate decay parameters (for example, the exponential decay rate for which the severity value will decrease to near zero over 1 month, 5 months, 1 year, 3 years, etc.).

Another advantage of the proposed study is that the PRIs selected for the study, even though they may only represent a small proportion of the total number of PRIs, have been selected methodically to address the individual and combined effects of PRI role type and PRI severity on judgments of PRI decay. It is hoped that this design will resolve issues that remained indeterminate based on the analyses and results of the initial study.

Empirical Study Incorporating the PRI Intent Ambiguity Factor

A study design identical to the one described in the previous section can be used to distinguish separate and combined effects of Role Type and PRI Intent Ambiguity on judgments of PRI decay.

The expert knowledge elicitation task would ask our expert analysts to judge the decay rates (none, low, medium, high) of different pairs of sixteen PRIs selected from the four role type categories, with two PRIs selected within each Role Type that have Ambiguous Intent and two that have Clear (malicious) Intent, as shown in Table 5. The PRIs used in the study need not be the same for all participants—different sets of PRIs may be used to the extent that representative Ambiguous Intent vs. Clear Intent PRIs may be identified.[6] The format of questions can be the same as described in Section Empirical Study of Role Type and Severity Factors, Figure 4.

Table 5. PRI Selections for two-Factor Study of Role Type and Intent Ambiguity

Role Type	PRIs with Ambiguous Intent	PRIs with Clear Intent
Personal Predisposition	PRI-1 PRI-2	PRI-3 PRI-4
Precipitating Event	PRI-5 PRI-6	PRI-7 PRI-8
Behavioral Precursor	PRI-9 PRI-10	PRI-11 PRI-12
Technical Precursor	PRI-13 PRI-14	PRI-15 PRI-16

A Three-Factor Study Design

The two study designs described in Sections Empirical Study of Role Type and Severity Factors and Empirical Study Incorporating the PRI Intent Ambiguity Factor do not consider a possible relationship between PRI Severity and PRI Intent Ambiguity. A cursory examination of such a relationship is revealed by comparing the severity scores for PRIs considered Ambiguous in Intent versus those considered to reflect Clear Intent: The mean severity scores for the 173 PRIs with Ambiguous Intent is 0.64; the mean of the 92 PRIs with Clear Intent is 0.82—the difference is highly statistically significant. Thus, PRIs with clear intent tend to have higher severity scores. A study design that examines all three factors would require twice the number of PRIs to be rated, as shown in Table 6. Note, however, that it may not be possible to fill all the cells/conditions in this study design: There are no Precipitating Events that reflect Clear Intent; there are very few (if any) Personal Predispositions that reflect Clear Intent (we included Mental Health Inpatient/Involuntary and Insanity Plea/Criminal Case as the only examples of such cases, and this may be debatable as to intent). Because the possibility of a 3-factor relationship is most applicable to Behavioral and Technical Precursors, a modified study design would only examine these role types, thereby eliminating half of the cases and producing a revised design with 16 PRIs (as indicated by the shaded portions of Table 6).

6 At the discretion of the experimenter(s), an expert knowledge study may be performed to pick representative Clear versus Ambiguous Intent PRIs within each role type category. This may not be necessary if the experimenters are confident in their ability to discriminate PRIs based on Intent Ambiguity.

Table 6. PRI Selections for Three-Factor Study of Role Type, PRI Severity, and PRI Intent Ambiguity

Role Type	PRIs with Ambiguous Intent		PRIs with Clear Intent	
Role Type	**PRIs with High Severity**	**PRIs with Low Severity**	**PRIs with High Severity**	**PRIs with Low Severity**
Personal Predisposition	PRI-1 PRI-2	PRI-3 PRI-4	PRI-5 *[PRI-6]*	PRI-7 *[PRI-8]*
Precipitating Event	PRI-9 PRI-10	PRI-11 PRI-12	*[PRI-13]* *[PRI-14]*	*[PRI-15]* *[PRI-16]*
Behavioral Precursor	PRI-17 PRI-18	PRI-19 PRI-20	PRI-21 PRI-22	PRI-23 PRI-24
Technical Precursor	PRI-25 PRI-26	PRI-27 PRI-28	PRI-29 PRI-30	PRI-31 PRI-32

Conclusions and Recommendations

The most important conclusion to be drawn from this analysis is that it is not feasible to do a definitive analysis and evaluation of possible PRI decay models with the data in hand. Additional expert knowledge elicitation tasks are needed. With the caveat regarding the limitations of the current analyses described in Section Limitations, a tentative/expedient rubric for assigning PRI decay rates was provided in Figure 3, based on the available data.

A recommendation that should be considered is to conduct a new expert knowledge elicitation study to further examine the possible contributions of role types, PRI severity, and PRI Intent in judgments of PRI decay characteristics. A different elicitation method (i.e., a different approach to asking questions about PRI decay) and some careful study design manipulations—as described in Section Proposed Empirical Study—may improve our understanding of how these factors influence PRI decay judgments.

Our current research and development effort is providing a new, expanded set of insider threat PRIs that is derived from the SOFIT PRI ontology [4] and current PRI lists defined by the US Department of Defense. This new PRI framework will require a new calibration of PRI strengths (severity values). Therefore, it is recommended that the expert knowledge elicitation exercises planned for the new PRI framework should also capture expert judgments of PRI decay. The study design proposed here for examining PRI decay can be incorporated into this larger calibration effort.

References

[1] Greitzer, FL, & J Purl. (2022). The dynamic nature of insider threat indicators. *Springer Nature Computer Science*, 3(102). https://doi.org/10.1007/s42979-021-00990-1. [online: accessed on September 30, 2022]

[2] Greitzer, FL. (2022). *Cogynt Insider Threat Indicator Decay Considerations*. White Paper. Cogility Software, Inc.: August 2022.

[3] Greitzer, FL, RA Kliner & S Chan. (2022). Temporal Effects of Contributing Factors in Insider Risk Assessment: Insider Threat Indicator Decay Characteristics. Paper presented at *ACSAC Conference Workshop on Research for Insider Threat (WRIT)*, Austin, TX, December 2022.

[4] Greitzer, FL, J Purl, YM Leong, & DE (Sunny) Becker. (2018). SOFIT: Sociotechnical and Organizational Factors for Insider Threat. In *2018 IEEE Security and Privacy Workshops*, San Francisco, CA, May 24, 2018.