IT@Intel White Paper

Intel Information Technology
Security
December 2009

Prioritizing Information Security Risks with Threat Agent Risk Assessment

Matt Rosenquist
Information Security Strategist, Intel IT

Executive Overview

Intel IT has developed a threat agent risk assessment (TARA) methodology that distills the immense number of possible information security attacks into a digest of only those exposures most likely to occur. This methodology identifies threat agents that are pursuing objectives which are reasonably attainable and could cause unsatisfactory losses to Intel.

The predictive output from TARA promotes informed decision making at every level of management by presenting complex information in a way that even audiences unfamiliar with information security can understand.

It would be prohibitively expensive and impractical to defend every possible vulnerability. By using a predictive methodology to prioritize specific areas of concern, we can both proactively target the most critical exposures and efficiently apply our resources for maximum results in information security risk management.

Specifically, the TARA methodology identifies which threat agents pose the greatest risk, what they want to accomplish, and the likely methods they will employ. These methods are cross-referenced with existing vulnerabilities and controls to pinpoint the areas that are most exposed. Our security strategy then focuses on these areas to minimize efforts while maximizing effect.

The TARA methodology offers several benefits:

- Awareness of the most exposed areas allows Intel to make better decisions about how to manage risks to an optimal level—balancing spending, preventing impacts, and managing to an acceptable level of residual risk.
- We can utilize company resources more efficiently and effectively because we maintain focus on the most critical risk areas.
- The predictive nature of TARA meshes well with our existing and continually evolving defense in depth strategy.
- The methodology is flexible and can readily adapt to changes in threat agents, computing environments, behaviors, and vulnerabilities.
- We can validate the accuracy of TARA predictions.

The predictive output from TARA promotes informed decision making at every level of management by presenting complex information in a way that even audiences unfamiliar with information security can understand. This provides us with company-wide support so we can manage Intel's information security risks to an optimal level.

Contents

IT@INTEL

IT@Intel is a resource that enables IT professionals, managers, and executives to engage with peers in the Intel IT organization—and with thousands of other industry IT leaders—so you can gain insights into the tools, methods, strategies, and best practices that are proving most successful in addressing today's tough IT challenges. Visit us today at www.intel.com/IT or contact your local Intel representative if you'd like to learn more.

Terms to Know

The following terms are used throughout this paper:

Vulnerability	Part of the information security infrastructure that could represent a weakness to attack in the absence of a control.
Threat Agent	Person who originates attacks, either with malice or by accident, taking advantage of vulnerabilities to create loss.
Motivation	Internal reason a threat agent wants to attack.
Objective	What the threat agent hopes to accomplish by the attack.
Method	Process by which a threat agent attempts to exploit a vulnerability to achieve an objective.
Attack	Action of a threat agent to exploit a vulnerability.
Control	Tools, processes, and measures put in place to reduce the risk of loss due to a vulnerability.
Exposure	Vulnerability without a control.

BACKGROUND

At Intel, information security is an important aspect of corporate risk management. It would be prohibitively expensive and impractical to protect the enterprise against every vulnerability, because information security attacks come in many forms, and attackers constantly evolve new tactics as we develop new defenses and controls. We need a way to identify the most likely attack vectors to support the development of optimal security strategies.

Early information security efforts in the IT industry concentrated on specific controls such as firewalls, virus scans, authentication and logon credentials, intrusion detection and prevention packages, and cryptography. These are important controls but are not easily sustainable as they rely on closing all emerging vulnerabilities. As the number of new vulnerabilities discovered each year has skyrocketed, this model of "fixing everything" becomes more costly while losing effectiveness—as soon as one hole is patched, two new holes appear. The information security industry has been searching for a rational method to narrow threats in a practical manner that can be applied to strategy, tactics, prioritization, and resource management.

Intel IT has developed a sophisticated approach to information security, our defense-in-depth strategy[1], which optimizes security using interlocking prediction, prevention, detection, and response capabilities. As part of our prediction capability, we have crafted a standardized threat agent library (TAL) that provides a consistent, up-to-date reference describing the human agents that pose threats to IT systems and other information assets.

Determining which types of attacks are possible is only the first step. The true value derives from knowing which attacks are most likely to occur.

1 See "Defense in Depth Strategy Optimizes Security," Intel Corporation, September 2008.

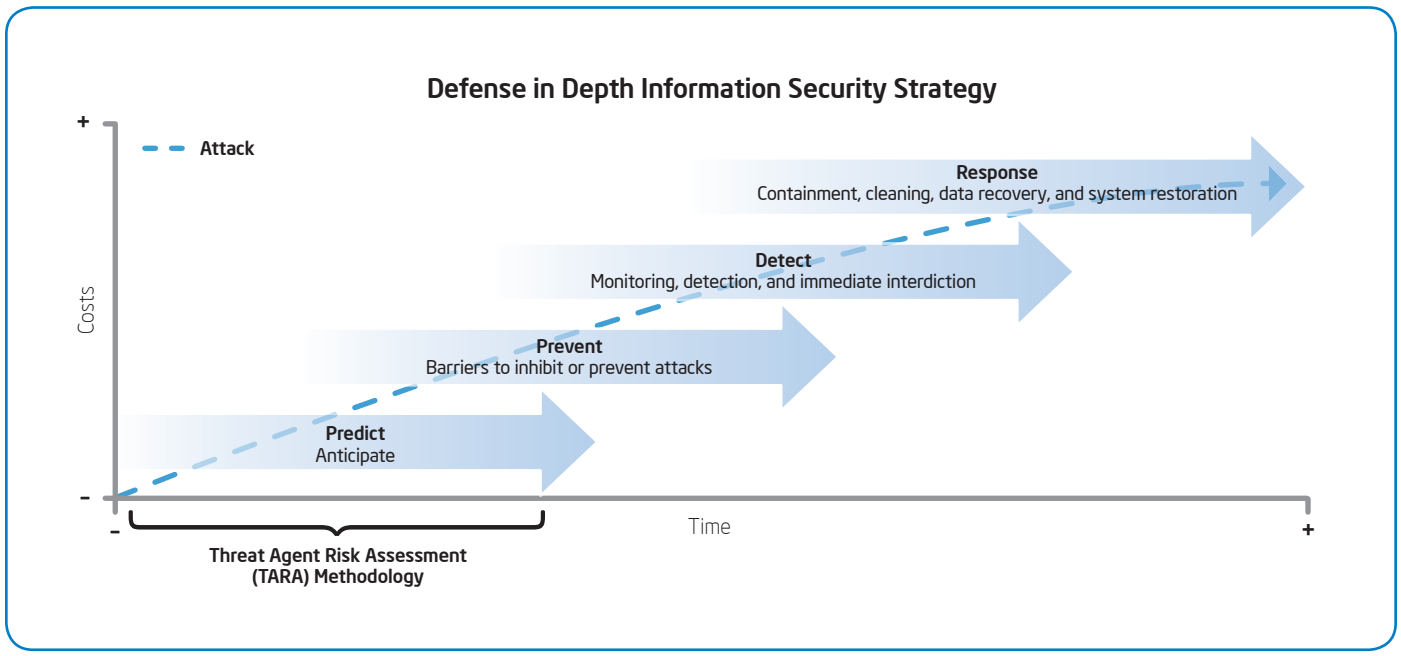

Figure 1. The threat agent risk assessment (TARA) methodology fits into the predict phase of our defense in depth information security strategy.

THREAT AGENT RISK ASSESSMENT

Just because a vulnerability is a possible target doesn't mean it is a probable one. Threat agent risk assessment (TARA) identifies the most likely attack vectors to support the development of optimal security strategies. TARA analysis enables us to pinpoint the information security areas of greatest concern—those which pose the highest level of overall risk.

These higher-priority areas are characterized by the existence of threat agents who have the motivation and capabilities to take advantage of likely methods that will lead them to their objectives—and will in turn cause unacceptable losses to Intel.

TARA methodology applies specifically to information security. We do not use it to predict the likelihood of other sorts of security risks such as theft of tangible goods. Nor is TARA a forensics tool for investigating specific incidents after they occur. Rather, TARA is a planning tool we use when we first start to consider risks in a certain area. TARA methodology is part of our overall defense in depth strategy, as shown in Figure 1.

TARA methodology is substantially different from vulnerability assessments. Vulnerability assessments attempt to identify every single weak point—but since virtually anything could be a weak point depending on the attacker, methods, and objectives, vulnerability assessments can never be comprehensive. Vulnerabilities are dangerous only if someone is interested in exploiting them and has the means to do it. TARA concentrates on threat agents and their motivations, methods, and objectives, and how they map to existing controls, not on the weak points themselves.

Figure 2 provides an overview of TARA methodology. Threat agents are attackers who represent a security risk of loss, and they are classified by characteristics including skills, capabilities, resources, intent, and access. For example, intent may be malicious or non-malicious. As the figure shows, threat agents are the origin of risks. A threat agent's motivations, capabilities, and objectives then map to likely methods. When a likely method intersects a vulnerability without controls, the result is an area of exposure. These resulting exposures, taking impacts into consideration, represent the most critical and high-priority areas of concern.

In addition to identifying the mostly likely exposures, TARA also takes into consideration acceptable levels of corporate risk. For example, if a successful attack is likely but poses very little potential for loss or damage, TARA does not identify it as a high-priority exposure.

The results of TARA analysis delineate the risks of greatest concern clearly, even to audiences who have little or no background in information security. This enables various levels of management to understand which information security risks are important, so

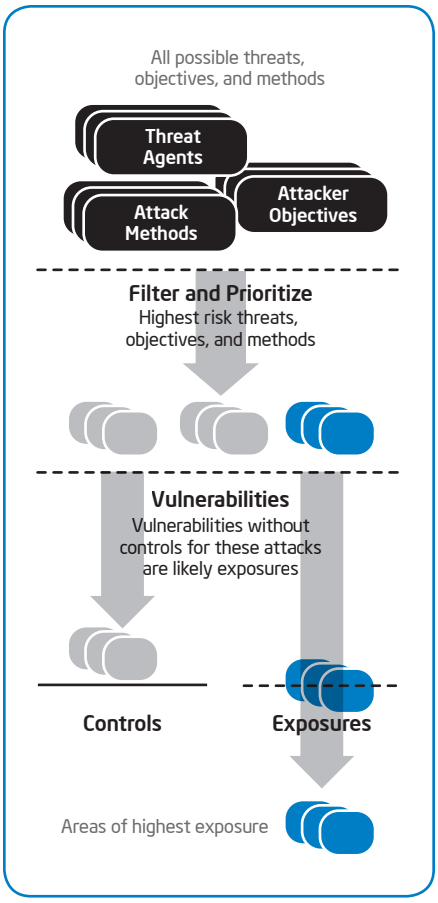

Figure 2. The threat agent risk assessment (TARA) methodology narrows the field of all possible attacks to determine the most likely attacks.

they can feed the results into a defense in depth strategy. This strategy includes:

- Control maps outlining specific preventative plans.
- Tactical monitoring plans to focus on likely successful attack vectors.
- Agent characterization in support of direct interdiction.
- Response plans to reduce specific impacts.

TARA Components

The TARA methodology relies on three main references to reach its predictive conclusions:

- Threat agent library (TAL)[2]
- Common exposure library (CEL)
- Methods and objectives library (MOL)

Standard frameworks such as these help ensure consistency and comprehensiveness when different risk assessors apply TARA methodology to different environments.

THREAT AGENT LIBRARY

The primary premise of the TARA methodology is that threat agents are the source of information security losses. Previously, Intel developed the TAL to simplify the character set of all possible threat agents. It was therefore a natural choice to use it with the TARA methodology.

The Intel TAL defines eight common threat agent attributes, such as intent—hostile or non-hostile—and access—internal or external. Based on unique combinations of these attributes, the TAL identifies 22 unique threat agent archetypes, such as disgruntled employee, competitor, and organized crime. It is important to remember that the TAL provides archetypes, not exact descriptions of real people; individuals may vary in degree of hostility from the model, for example.

COMMON EXPOSURE LIBRARY

For the first application of the TARA methodology, we created our own CEL, which enumerates known information security vulnerabilities and exposures at Intel. There are also several publicly available CELs that provided additional data for ours.

The CEL maps our vulnerabilities against existing controls to show which exposures are residual. For example, because we have an antivirus solution installed on corporate laptop PCs, currently known viruses do not represent an overt exposure. However, if an unknown virus appears before we have updated the antivirus solution, then an appreciable residual exposure exists.

METHODS AND OBJECTIVES LIBRARY

The third component of TARA, the MOL, lists known threat agent objectives—what they want to accomplish—and the most likely methods they will employ to reach these objectives. These methods and objectives are cross-referenced with our defense-in-depth controls, such as firewalls, proxies, secure device configurations, and a security-aware workforce. Table 1 shows a sample subset of our MOL.

When the MOL is coupled with the TAL, a picture begins to emerge of the types of likely possible attacks, based upon many factors such as resources, objectives, typical methods, and preferred vulnerabilities. Additionally, an estimate of consequences begins to form. When the CEL is overlaid on this picture, those vulnerabilities with sufficient controls aligned to reduce risk are dropped, and the remaining vectors of attack emerge as the areas of highest exposure.

2 See "Threat Agent Library Helps Identify Information Security Risks," Intel Corporation, September 2007.

Table 1. Sample from Methods and Objectives (MOL) Library

AGENT NAME	ATTACKER					OBJECTIVE		METHOD								IMPACT				
	Access	Trust				Motivation	Goal	Acts					Limits							
		None	Partial Trust	Employee	Administrator			Copy, Expose	Deny, Withhold, Ransom	Destroy, Delete, Render Unavailable	Damage, Alter	Take, Remove	Code of Conduct	Legal	Crimes Against Property	Crimes Against People	Loss of Financial Assets	Business Operations Impact	Loss of Competitive Advantage, Market Share	Legal or Regulatory Exposure	Degradation of Reputation, Image, or Brand
Employee Error	Internal		X	X	X	Accidental/Mistake	No malicious intent, accidental	X		X	X		X				X	X	X	X	X
Reckless Employee	Internal		X	X	X	Accidental/Mistake	No malicious intent, accidental	X		X	X			X			X	X	X	X	X
Information Partner	Internal		X			Accidental/Mistake	No malicious intent, accidental	X		X	X						X	X	X	X	X
Competitor	External	X				Personal Gain (Financial)	Obtain Business or Technical Advantage	X							X				X		
Radical Activist	External	X				Social/Moral Gain	Change Public Opinion or Corporate Policy	X	X	X	X	X				X		X			X
Data Miner	External	X				Personal Gain (Financial)	Obtain Business or Technical Advantage	X							X				X		
Vandal	External	X				Personal Gain (Emotional)	Personal Recognition or Satisfaction			X	X				X			X			X
Disgruntled Employee	Internal		X	X	X	Personal Gain (Emotional)	Damage or Destroy Organization		X	X	X				X			X	X		X

The TARA Process in Detail

To find the critical areas of exposure, the TARA methodology uses six steps.

1. **Measure current threat agent risks to Intel.** Using the TAL, a panel of senior Intel experts regularly reviews and ranks the current threat levels at Intel. This is a qualitative to quantitative exercise necessary to establish a general understanding of current risks, and it creates a baseline for future TARA exercises.
2. **Distinguish threat agents that exceed baseline acceptable risks.** Again using the TAL, we measure new threat levels if we're starting a new project, or we create an acceptable risk baseline if we don't think the current baseline is sufficient. At the end of steps 1 and 2, we have identified the threat agents that exceed the current or new baseline threat level for the areas being evaluated.
3. **Derive primary objectives of those threat agents.** TARA defines objectives as the combination of threat agent motivations and threat agent capabilities. Using the MOL, we derive the primary motivations and objectives of those threat agents identified in steps 1 and 2. Motivations are important because they underpin action, and they contribute to factors such as the attacker's commitment, the point at which attacker will cease pursuit, and the attacker's susceptibility to targets of opportunity. Table 2 lists some examples of threat agent objectives.
4. **Identify methods likely to manifest.** Again using the MOL, we identify the likely methods by which an attack may occur. TARA defines a method as a combination of threat agent objectives and threat agent operating methods. TARA identifies the type of impact we could expect based on motivations and objectives.
5. **Determine the most important collective exposures.** Using the CEL, the methodology first finds attack vectors, which are vulnerabilities without controls. Then, the intersection of the methods determined in step 4 and the attack vectors define likely exposures. Finally,

Table 2. Examples of Threat Agent Objectives

OBJECTIVE	EXAMPLE
Theft/Exposure	Exposure of data resulting in loss of competitive advantage, including loss of intellectual property and personal data.
Data Loss	Destruction or alteration of data—including corruption, tampering, denial of access, and deletion—so it is not usable or it loses value.
Sabotage	Willful and persistent attempt to cause disruption and damage, including destruction of systems, capabilities, processes, designs, and brand.
Operations Impact	Negative impact on business operations, including manufacturing, research, and engineering.
Embarrassment	Embarrassment targeted at individuals or the corporation, including real and fabricated defamation, reputation poisoning, and harassment targeting specific personnel or the corporation.

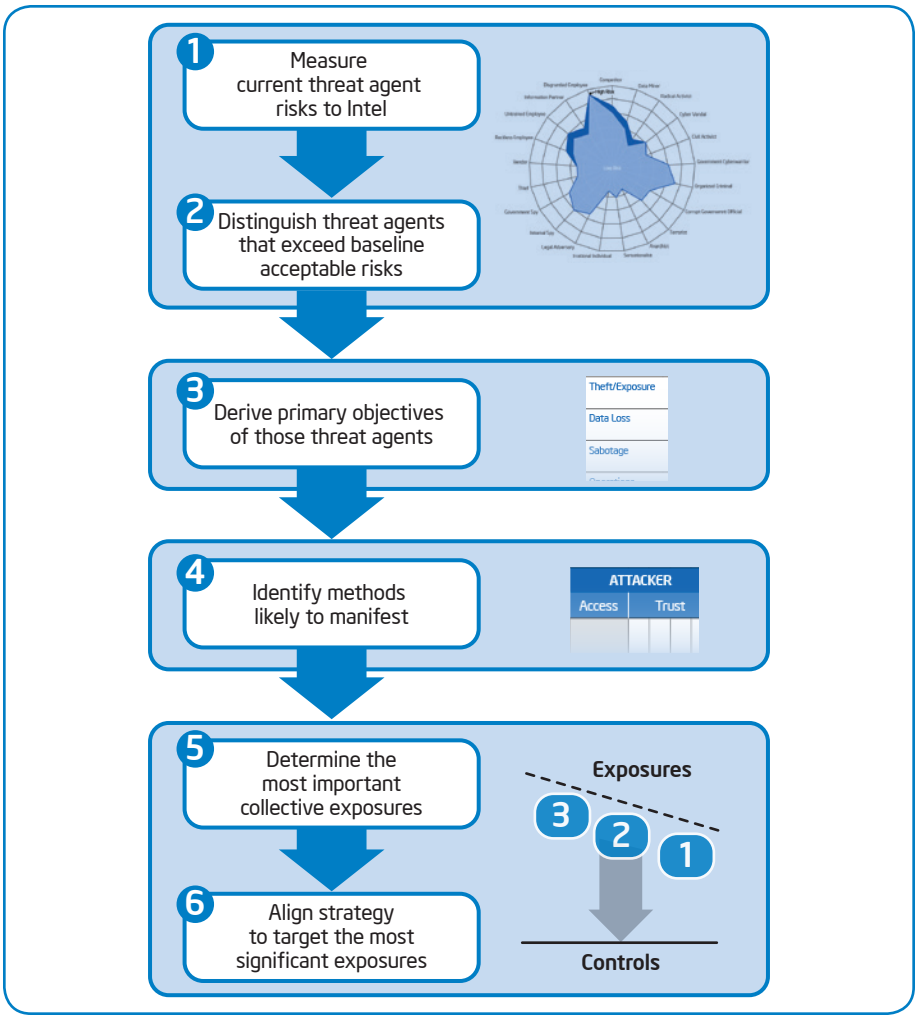

Figure 3. By identifying the most important threat agents, objectives, and methods, the threat agent risk assessment (TARA) methodology can help align our information security strategy to the most critical exposures.

these likely exposures are ranked according to their severity of consequence. The end result of step 5 is a list of the most important collective exposures.

6. **Align strategy to target the most significant exposures.** An assessment is worthless if it does not reinforce the decision-making process. Analysts and management can use the results of TARA analysis to concentrate their information security strategy on the most important areas of concern and allocate information security resources in the most effective manner.

Figure 3 shows these steps in action, including a sample of TARA output at each stage. As the figure illustrates, the output uses graphs and tables to clearly communicate the areas of greatest information security risk.

Results

Figure 4 shows one hypothetical example of the type of risk assessment data TARA can provide when assessing information security risks associated with a particular project. The very center of the diagram represents low risk, and the risk level increases toward the outer rim of the circle. The light blue area

Department of Homeland Security Adopts Intel's Threat Agent Library

In May 2007, the U.S. Department of Homeland Security (DHS) published the Information Technology Sector-Specific Plan, which provides guidance on how public and private entities will work together to protect IT infrastructure in the United States.

In August 2009, the DHS and the Information Technology Sector Coordinating Council released the IT Sector Baseline Risk Assessment (ITSRA) to identify and prioritize national-level risks to critical, sector-wide IT functions while outlining strategies to mitigate those risks and enhance national and economic security.

The ITSRA, which incorporates Intel's threat agent library (TAL) as the foundation of its methodology, validates the resiliency of key elements of U.S. IT infrastructure while providing a process by which public- and private-sector owners and operators can continually update their risk management programs. The assessment links security measures to concrete data to provide a basis for meaningful infrastructure protection metrics.

For more information on the ITSRA, visit www.dhs.gov/xlibrary/assets/nipp_it_baseline_risk_assessment.pdf.

represents default risks; these risks existed before the project began. In some situations they may represent accepted risks per company policy. The dark blue areas show the elevated risks associated with the project. For example, in Figure 4, "irrational individuals" do not present a major threat during this project, while "disgruntled employees" are one of the highest risks.

We tested and successfully applied TARA methodology to a very large project, which we then studied to determine TARA's effectiveness. This project posed direct significant risks to many areas of Intel operations, including our supply network, high-speed manufacturing, product design engineering, product assembly and test, enterprise applications, and IT systems.

During this project, corporate policy and normal controls managed the default risks; using the TARA results, we could focus on the risks specific to the nature of the project. To derive the highest priority residual exposures, we overlaid the areas of concern from the TARA analysis against existing information security controls, and we were able to develop an overall information security strategy for the project.

Confidence in any risk assessment methodology is based upon its accuracy. TARA is predictive in nature and outlines the likely attacks and consequences. If we establish controls to reduce the risk of a successful attack, the consequences may not actually occur. However, the attack attempts can be apparent, and we can track them. Evaluating the predicted likely attack vectors against what actually occurs is one way to measure relative accuracy. In our case study, as the project progressed over two years, the areas of concern highlighted by the TARA analysis proved to be accurate predictors of likely attack vectors.

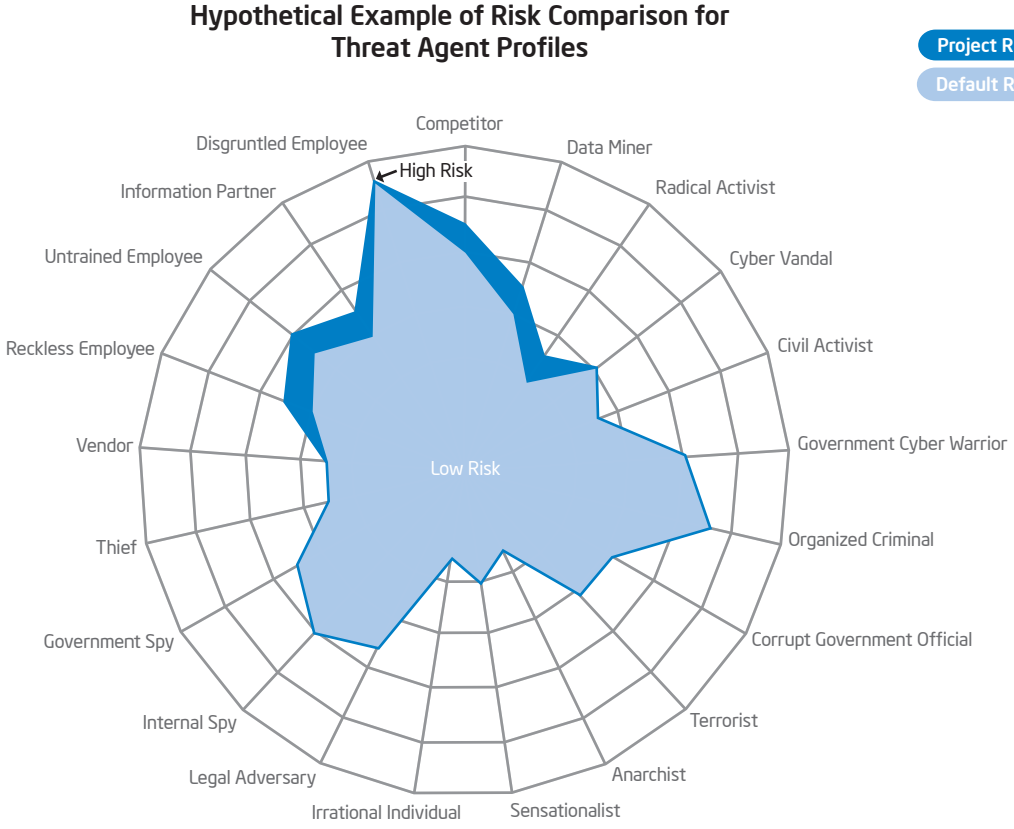

Figure 4. The threat agent risk assessment (TARA) methodology provides information on project-specific information security risks, which may differ from an organization's default level of information security risks.

CONCLUSION

TARA is a new direction in information security risk assessment. It distills an overwhelming risk landscape to the most likely risks, so an organization can properly align resources and intelligently develop an ongoing security strategy.

TARA methodology has several characteristics that make it attractive to managers who may view information security as too complex and complicated:

- **Sensible.** TARA narrows the number of threat vectors to those most likely to occur, thereby reducing the threat surface we must protect, and communicates this information in an easy-to-understand format.
- **Adaptive.** TARA can adjust to changes in threat agents, attack methods, and attacker objectives.
- **Comprehensive.** TARA covers all types of security incidents, including internal and external; malicious and non-malicious; and direct and indirect.
- **Scalable.** TARA methodology is applicable to any size organization at any level of complexity.
- **Practical.** TARA methodology can be as quick and simple or as deliberate and complex as needed.
- **Rational.** TARA's predictive results can be validated over time and provide support for trend analysis and risk exposure snapshots.

These characteristics contribute to TARA's major strengths, which include:

- The ability to analyze and prioritize the most important risks, and then summarize them into a narrow set of likely attacks representing the areas of greatest information security concern.
- The ability to effectively communicate analysis results across management levels. Even audiences unfamiliar with information security can understand the results of a TARA analysis, because TARA's filtering methodology reduces complex, seemingly chaotic data to something more manageable.
- Cross-referenced with controls to show the true level of exposure.
- Takes into account acceptable risk levels.
- The ability to validate its predictive results over time.

By adapting to the constantly changing landscape of threat agents, objectives, and methods, TARA allows us to make better decisions on how to manage information security risks at an optimal level, properly allocating resources and balancing spending against prevented losses.

ACRONYMS

CEL	common exposure library
DHS	Department of Homeland Security
ITSRA	IT Sector Baseline Risk Assessment
MOL	methods and objectives library
TAL	threat agent library
TARA	threat agent risk assessment

For more straight talk on current topics from Intel's IT leaders, visit www.intel.com/it.

Printed in USA
1209/JLG/KC/PDF

Please Recycle
322696-001US