

IT@Intel

Understanding Cyberthreat Motivations to Improve Defense

We have added a new parameter to our threat taxonomy—Motivation—to describe the typical motivation of classes of threat agents.

Threat-based risk management is a highly effective strategy to identify, assess, prioritize, and control cybersecurity risks.

Executive Summary

As part of a robust defense-in-depth strategy, Intel approaches cybersecurity from both a proactive and reactive position. Reactively, we actively monitor developments in malware and its ecosystems and have mature processes for dealing with malware and other threats found in our computing environment. Proactively, we pay close attention to the types of attackers who might target our assets, areas where they are active, and trends and developments in their methods. This approach enables our designers and defenders to better allocate finite defensive resources in the most effective manner.

When investigating an actual incident, specific individuals or organizations responsible for the attack must be identified and described in a straightforward way to aid remediation and, where appropriate, assist law enforcement action. These techniques, employed reactively, are well understood and practiced throughout industry and law enforcement. Proactive efforts, on the other hand, are relatively new and lack effective tools. To aid our proactive efforts we developed a taxonomy to comprehensively and uniformly describe agents of threat. These descriptions focus on *classes* of attackers to help predict what a member of that class might typically do to cause harm, before it happens. We published this taxonomy and a Reference Library of characters^{1,4} for public use in 2007.

We are now adding a parameter that describes the typical motivations of classes of threat agents. The new *Motivation* parameter identifies the driver—be it emotional or the pursuit of supremacy or material gain—that causes the threat agent to commit harmful acts. Understanding these drivers is important because when applied to a threat agent in context, the Motivation elements help indicate the nature of the expected harmful action. We believe this understanding is also crucial in understanding how to correctly evaluate organizational activity, as it often differs greatly from the people working for that organization.

As used in our taxonomy, the word “Motivation” includes items beyond the strict definition of an emotional state, expanding it to comprehensively describe the full range of human threat. While any combination of these elements could drive any individual to commit malicious acts, these elements are used to describe the *primary* motivations of a threat agent *class*.

Table of Contents

- Executive Summary1
- Why We Are Now Including Motivation ...2
- The Motivation Parameter3
 - Assigning Motivations to Threat Agents3
 - Group Causes versus Personal Motivators for Individuals5
- Elements of the Motivation Parameter ...5
 - Accidental.....5
 - Coercion5
 - Disgruntlement.....6
 - Dominance.....6
 - Ideology6
 - Notoriety.....6
 - Organizational Gain6
 - Personal Financial Gain.....7
 - Personal Satisfaction.....7
 - Unpredictable.....7
- Appendix: Motivation Assignment.....8

Why We Are Now Including Motivation

By design, our original taxonomy did not include motivations. At the time, we believed that whether the attack was for fame or for money, it did not change our defense strategies and would not affect our analysis or planning. However, as we started applying agent analysis methods, such as in the Threat Agent Risk Assessment (TARA) methodology,² we realized that motivation actually has a significant impact on defense planning (Figure 1). Threat agents are human, and fully understanding their threat requires understanding what human drives are involved. This understanding enables defenders to design more tailored controls and perhaps even mitigate the threat itself, such as intercepting a disgruntled employee with counseling before the situation becomes harmful.

With this realization, we now include Motivation in our taxonomy, for several reasons:

- Knowing a threat agent’s motivation narrows which targets that agent may focus on. For example, Mobster agents, who have a strong profit motive, will generally only take assets they can easily convert to cash regardless of the discoverability of their actions, while agents seeking notoriety will ignore attacks on non-visible assets that will not bring them attention.

- Understanding the agents’ intent helps defenders focus their often-limited defense resources on the most likely attack scenarios for any particular asset.
- Motivation shapes the intensity and the persistence of an attack. Threat agents usually act in a manner that reflects their underlying emotion or situation, and this informs defenders of the manner of attack. For example, a spy motivated by nationalism (Ideology) likely has the patience to achieve long-term goals and work quietly for years, whereas a cybervandal out for kicks can create an intense and attention-grabbing attack but quickly loses interest and moves on. Understanding these differences allows defenders to implement controls tailored to each type of attack for greatest efficiency.
- Motivation helps in describing threat and risk scenarios in less technical terms. Analysts must eventually convey all agent analysis to others in their organization who can act to help mitigate the risks. Describing Motivation tells a fuller, more relatable story to colleagues of all security levels. Communicating risks in a more understandable fashion obviously leads to faster implementation of more effective defenses.

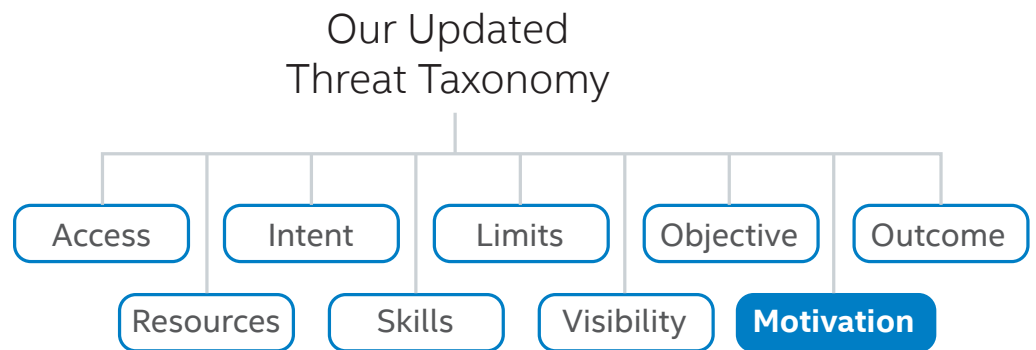


Figure 1. We added Motivation to our threat taxonomy after realizing that it has a significant impact on defense planning.

The Motivation Parameter

When applied to threat agents, the word “motivation” can have two meanings: *cause*, the reason a person commits an act, or *drive*, which describes the level of interest or intensity a person acts on. We use both meanings in our application of the Motivation parameter. Primarily, the Motivation parameter describes *cause*, the emotional or situational reason the agent has taken a harmful action. However, those harmful actions may be unintentional, so the Motivation parameter does not necessarily signify hostile intent.

Regarding *drive*, we always assume agents are working at a high interest level; otherwise, they would probably not pose enough threat to warrant attention. However, the intensity and the duration of a highly driven individual can vary widely, and this second facet of the Motivation parameter attempts to give insight into the typical attack profile.

We have defined 10 elements for the Motivation parameter: Accidental, Coercion, Disgruntlement, Dominance, Ideology, Notoriety, Organizational Gain, Personal Financial Gain, Personal Satisfaction, and Unpredictable.

Gain, Personal Financial Gain, Personal Satisfaction, and Unpredictable (Figure 2). This set of elements describes all the major motivations relevant for describing threat. Like the other parameters in the threat agent taxonomy, each element is independent of the others; that is, there are no direct linkages between them, and there is no minimum or maximum number of agents they may be assigned to. Each element is described in the [Elements of the Motivation Parameter](#) section.

Assigning Motivations to Threat Agents

Our team held many working sessions over several months to research and develop the Motivation parameter and its elements. We originally started with four elements and hoped each of our Reference agents would fall neatly into only one of those elements. But as we worked to develop and assign the Motivations, we discovered that describing the agents sufficiently required not just a larger set of elements, but also adding modifiers to capture the nuances necessary to portray them in a recognizable human picture.

60% DECREASE

in risk management time by defining threats concisely and consistently across the organization.



Figure 2. We have defined 10 elements for the Motivation parameter.



“The inability to define our enemy is the reason we deal with consequences instead of root causes.”

–Special Agent Kim Jensen, FBI terrorist profiler

For each agent, we describe several motivational aspects using elements of the Motivation parameter (Figure 3).

- **Defining.** The archetypical, single most prevalent and descriptive motivation of this agent class. This motivation is intrinsic to the agent and the primary cause of the agent's actions (as a class). A small number of individuals may actually have a different motivation, but for proactive threat agent analysis this motivation is used as the analysis basis.

The Defining Motivation is assigned to all agents and is the only aspect required to define an agent. The following modifiers are optional and may or may not apply to any particular subgroup or individual in that class:

- **Co-motivation.** A motivation that can exist as an equal or near-equal cause to the Defining Motivation. It does not replace or magnify the Defining Motivation, but might indicate additional asset or attack targeting. For example, Mobsters have a Defining Motivation

of Organizational Gain, which is the primary cause of their actions. However, they may also use the same actions to establish Dominance, which is a form of competitive advantage in many organized crime domains and must be constantly reinforced.

- **Subordinate.** A subcategory to the Defining Motivation, providing additional insight into nuances that may influence different groups within the agent class. For example, a cybervandal, such as a hacktivist, is primarily seeking Dominance, but may also derive excitement from the lawlessness of the acts, making Personal Satisfaction an additional motivation for that subgroup.
- **Binding.** Describes the motivation that brings an individual into an organization in the agent class. Usually aligns with the Organizational Gain motivation but is often different from the Personal Motivation (the primary cause for an individual acting within an organization).

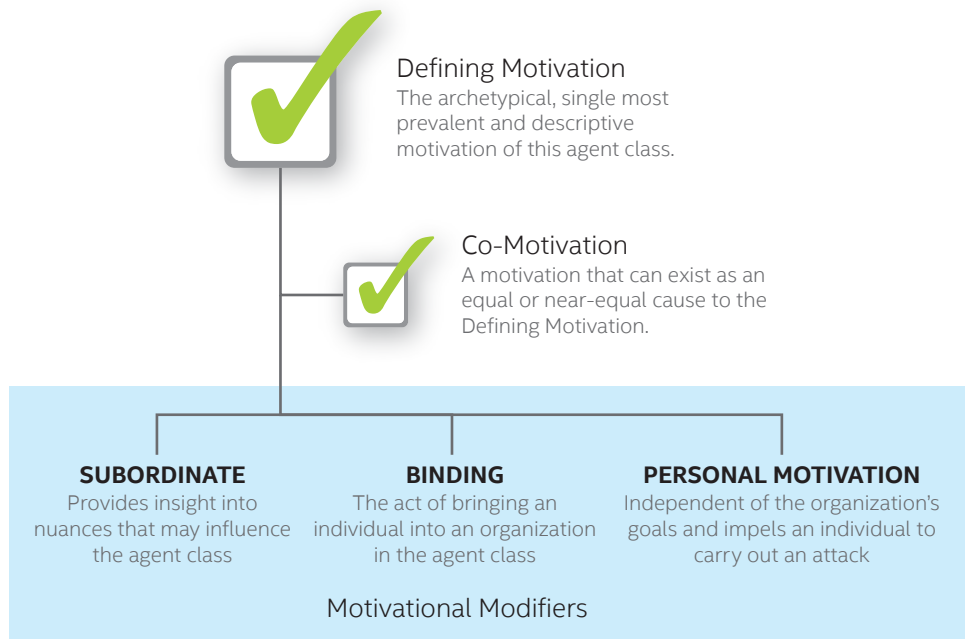


Figure 3. Motivational aspects help describe agents, and adding modifiers provides insight into nuances that create a recognizable human picture.

Group Causes versus Personal Motivators for Individuals

During the development of the Motivation parameter, we were surprised to discover the degree of significance to our agent analysis in the difference between what motivates an organization as a whole and what motivates an individual working for that organization. While the organizational motivation defines the cause and consequently the targeting, *the individual's personal motivation directly and significantly influences the actual harmful action defenders must prepare for, often irrespective of the host organization's motivation.* This was an important understanding, because it may explain why previous attempts at assigning motivations to organizations did not accurately predict the organization's actual attack activities.

To capture this important distinction between the organizational and individual motivators, we created an additional modifier—Personal Motivation—to allow analysts to specify both motivations for a single agent. In many cases an analyst must consider both equally to fully assess the agent's threat.

Personal Motivation, which is independent of the organization's goals, describes what impels an individual to carry out an attack. Personal Motivation may align with the organization's motivation—as is common with activists—but more often it supports personal objectives. For example, an individual analyst may join a Data Miner corporation because his or her values and skills align with the corporation's objectives. But the analyst most likely performs his or her daily work toward those objectives for personal reward in the form of a paycheck. The motivation of personal reward may be even stronger for agents who commit illegal acts, as it is more difficult for someone to cross that line purely for altruistic reasons.

Elements of the Motivation Parameter

The following are descriptions of the 10 elements we defined for the Motivation parameter.

Accidental

Benevolent or harmless intent but with actions that inadvertently cause harm

This element generally describes the non-hostile agent, such as a well-meaning, dedicated employee who through distraction or poor training unintentionally causes harm to his or her organization. A common occurrence is an employee who was quickly assigned additional duties to cover for laid-off employees but has not yet received proper training. With a heavy workload and lacking a full understanding of the tasks, the employee is bound to make mistakes, unwittingly and possibly without even knowing a mistake has occurred.

Coercion

Forced to act illegally on behalf of another

Unlike the other Motivations, a coerced person does not act for personal gain, but out of fear of incurring a loss. These individuals have been forced through intimidation or blackmail to act for someone else's benefit and are conducting acts they probably would not normally do and that may even directly conflict with their own self-interests. In most cases, a coerced person is just as much a victim as the attack target.

Coercion can effectively force a person to commit very harmful, possibly violent actions, if the threat against him or her is severe enough. Coercion can also subvert employees often considered above reproach, such as executives or those who undergo regular security checks. However, this element will typically be short-lived, as it is generally more difficult—although certainly not impossible—to force someone to commit illegal acts for an extended period.

There are probably fewer total threat agents driven by Coercion than by the other Motivations, but it can be a motivator for almost any kind of threat and must be considered when planning for risks. However, because of the general low incidence and non-specificity of Coercion, we list it in our Motivations mapping ([Appendix: Motivation Assignment](#)) only in places where we believe the probability of Coercion may be significantly increased.

Personal Motivation is independent of the organization's goals and describes what impels an individual to carry out an attack.

Disgruntlement

A desire to avenge perceived wrongs through harm

Most people go through stages of dissatisfaction with their employer or with a company they have done business with, but usually the situation resolves without illegal behavior. When the grievance (real or perceived) is severe and the situation escalates, a disgruntled person can seek revengeful and harmful retaliation. Unlike Ideology, Disgruntlement implies there is a history of some direct interaction with the target organization.

Disgruntled threat agents can include employees or former employees, all of whom may have extensive knowledge that the agents can leverage when conducting attacks. Often a Disgruntled individual acts alone but may join an organization, whether a competitor, group of similar individuals, or criminal organization, if the individual believes that doing so will enable him or her to better harm the source of his or her anger.

Predicting the actions of a disgruntled person or group is very difficult, because the action can take many forms including sabotage, violence, theft, fraud, or embarrassing individuals or the organization.³

Dominance

Attempting to assert superiority over another

Dominance can take many forms at many scales, for example, physically intimidating a coworker, threatening to expose sensitive data of a corporation, or amassing an army along a border. But in all cases threat agents use whatever power they have to bully others into submission.

Threat agents seeking dominance may also steal information assets to create power and build toward a goal of dominance. Collection can include compromising items such as sensitive intellectual property, personal information, business data, product data, and information on operational aspects such as networks and supply chains. Access to these items allows an attacker to leverage them or their vulnerabilities during an attack. For example, to prepare for a cyberattack

during a future national conflict, a government spy may steal software bug reports from a network device manufacturer, which detail the device's vulnerabilities and enable cyberattacks.

Ideology and Dominance may both be present in some state-sponsored agents, but Dominance can occur with or without Ideology. Mobsters often act to establish dominance in extreme acts of bullying but not in support or in conjunction with some higher objective—that is, Ideology.

Vandalism and hacking are also included under Dominance, because cybervandals typically seek dominance over others through bullying. Other factors, such as Notoriety, may also be present to some degree in these agents, but Dominance is the primary motivator.

Vandalism and hacking are included under Dominance, because cybervandals typically seek dominance over others through bullying.

Ideology

A passion to express a set of ideas, beliefs, and values that shapes and drives harmful acts

Threat agents who act for ideological reasons are not usually motivated primarily by the desire for profit; they are acting on their own sense of morality, justice, or political loyalty. Ideological motivation can arise independent of any prior interaction with the target. For example, an activist group may sabotage a company's equipment because they believe the company is harming the environment even though they may have never actually used any of the company's products.

Because ideologies vary, so do the types of threat posed by individuals or organizations with this motivation. The threat may come in the form of a direct attack, such as sabotage, theft, or exposure of sensitive information. It may also happen indirectly, such as an employee who improperly uses company

computers to participate in a cyberattack against an organization the employee believes to be oppressive. If traced back, the attacked organization could launch a counterattack or bring legal action against the unsuspecting "attacking" company.

Notoriety

Seeking to become well known for harmful activity

Threat agents motivated by Notoriety are often seeking either personal validation or respect within a community. The actions used to achieve even unreasonable notoriety may be quite well reasoned and strategic. Similar to vandalism, the individual or group may seek to cause damage for its own sake, but staying covert is not a priority—quite the opposite, in fact. To garner the respect of their target audience, the actions that those seeking notoriety take are not tempered by a need for secrecy and therefore can be extreme in scope and damage.

Organizational Gain

Seeking an advantage over a competitor's organization

The prospect of increased profit or other gains through an unfairly obtained competitive advantage has always been a powerful incentive, and the temptation to cheat will always be too strong for some to resist. Through theft of information such as intellectual property, business processes, or supply chain agreements, a competitor bypasses the lengthy and expensive process of developing it themselves, accelerating its position in a market or capability. The inappropriate acquisition or misuse of information, even seemingly esoteric data such as employee demographics, could be used to gain a competitive edge.

Information theft is not the only option used to get ahead. A competitor could also choose sabotage, lawsuits, or other non-theft means to undermine a competing organization to gain an advantage.

Organizational Gain includes military objectives as well. A military organization can use stolen information to advance its own technology while also enabling careful study of their target's capabilities and vulnerabilities.

In some cases, individuals with similar objectives may work collaboratively to advance their own personal gain but do so under voluntary organizational rules, such as military mercenaries or hacktivist collectives. In these cases, the organization motivation reflects the individuals' motivation (see the [Personal Motivation modifier in the Group Causes versus Personal Motivators for Individuals](#) section).

Personal Financial Gain

Improve one's own financial status

A selfish desire for personal gain motivates many crimes. This element describes individuals who steal money in some way or conduct activities that will net them money, such as hacking in exchange for a paycheck. These individuals are most likely indifferent to the damage caused by their actions, but apart from stealing, usually do not go out of their way to harm their target.

This motivation is different from Organizational Gain in the timeliness of the threat. Usually, the individual stealing assets wants to make a quick profit by selling them, rather than invest the time and expertise needed to craft a package for sale like an organization might create. Financial fraud is a result of this motivation, as is physical theft of valuable items. Intellectual property theft for sale is also a result of this motivation, but in the special case of espionage, Ideology may also play a significant part in an individual's motivation (see the [Co-motivation modifier in the Assigning Motivations to Threat Agents](#) section).

An individual threat agent may be seeking personal gain, but this does not mean that the agent always acts alone. Many criminal groups, organized or not, are often made up of individuals banded together solely to maximize their own personal profits.

In addition to greed, the need to steal can stem from other factors, such as pressing medical or addiction debts, poverty, coercion, disgruntlement, or mental impairment. These issues can easily lead an otherwise honest individual to commit illegal acts.

Personal Financial Gain can also apply to individuals working for an organizational threat agent, such as a Competitor or Mobster/Organized Crime. While the organization seeks an advantage for its collective goals, the individuals working for that organization may be driven by more personal reasons that may have little to do with the organization's objectives. Often this personal motivation is simply the personal financial gain that results from supporting the organization, such as a paycheck or a cut of the spoils. (See the [Personal Motivation modifier in the Assigning Motivations to Threat Agents](#) section).

Personal Satisfaction

Fulfilling an emotional self-interest

Some people may cause harm when they act not to support a financial or ideological objective but to satisfy a strictly internal, personal interest. This personal interest can be expressed in many ways, such as intrusive curiosity or thrill seeking, like children who break into a building just for the excitement of going where they are not allowed. More harmful possibilities include a healthcare worker who inappropriately reads the medical records of celebrities to see what treatment they are receiving or a hacker who attacks a website primarily because he or she enjoys the lawlessness of the act. Most "crimes of passion"—those caused by love, anger, fear, and so on—also fall under Personal Satisfaction.

Threat agents driven by Personal Satisfaction may incidentally receive some other gain from their actions, such as a profit, but their primary motivation is to gratify a personal, emotional need. This personal interest does not preclude people from banding together with other like-minded individuals toward a mutual, but not necessarily organizational, objective.

Unpredictable

Acting without identifiable reason or purpose and creating unpredictable events

It may seem that since Unpredictable represents the actions one cannot anticipate, there is no need to include

it—everyone knows life has many surprises. However, explicitly recognizing the potential for unpredictability in an environment and comprehending it in planning is essential for effective risk management. We include Unpredictable here to enable and support the discipline of planning for the unexpected.

In its application as a threat agent Motivation, Unpredictable is not a miscellaneous or default category. It does not include acts such as a sudden DDOS attack on a company website or a new type of email phishing campaign. Those events may have occurred unexpectedly and the methods may have been novel, but a reasonable person could easily anticipate those kinds of events would occur at some point. In this taxonomy, Unpredictable means a truly random and likely bizarre event, which seems to have no logical purpose to the victims.

In many cases Unpredictable acts will be the actions of a mentally disturbed person, such as the near-assassination of U.S. President Ronald Reagan in 1981 by a man who acted not for political reasons but because he believed his act would attract the love of a movie actress he had never met. Unpredictable acts can also come from competent agents with a new or unanticipated purpose. For example, in 2012 a small anarchist group began shooting at scientists employed at various nanotech companies. (Several people were injured but no one was killed.) The anarchists targeted them because they believed the scientists were working on implantable microcircuits that governments could use to monitor the thoughts of its citizens.

For our purposes, it is not the anarchists' misguided conclusions that make them Unpredictable in an analysis, but in acting so violently against a target no one expected. To them, their conclusions were perfectly rational and their actions reasonable for the situation. To the security managers of those companies—who probably had anticipated and prepared for physical threats to the CEO and other corporate officers—the extreme ambush attacks on presumably lesser targets were not practically foreseeable and so would fall into the Unpredictable motivation.

Appendix: Motivation Assignment

MOTIVATIONS OF THE REFERENCE LIBRARY OF THREAT AGENTS ⁴					
REFERENCE AGENT LABEL	DEFINING MOTIVATION	CO-MOTIVATION	SUBORDINATE MOTIVATION(S)	BINDING MOTIVATION	PERSONAL MOTIVATION
Civil Activist	• Ideology		• Organizational Gain	• Ideology	• Ideology
Radical Activist	• Ideology		• Dominance • Organizational Gain	• Ideology	• Ideology
Anarchist	• Ideology	• Unpredictable		• Ideology	• Ideology
Competitor	• Organizational Gain			• Organizational Gain	• Personal Financial Gain
Corrupt Government Official	• Personal Financial Gain				• Personal Financial Gain
Cybervandal	• Dominance		• Personal Satisfaction	• Dominance	• Dominance
Data Miner	• Organizational Gain			• Organizational Gain	• Personal Financial Gain
Disgruntled Employee	• Disgruntlement	• Personal Satisfaction	• Dominance • Ideology • Personal Financial Gain		• Disgruntlement
Government Cyberwarrior	• Dominance			• Dominance	• Ideology • Personal Financial Gain • Personal Satisfaction
Government Spy	• Ideology			• Ideology	• Ideology • Personal Financial Gain • Personal Satisfaction
Internal Spy	• Personal Financial Gain	• Ideology		• Personal Financial Gain	• Coercion • Ideology • Personal Financial Gain
Irrational Individual	• Unpredictable				
Legal Adversary	• Dominance			• Dominance	• Personal Financial Gain • Notoriety
Mobster	• Organizational Gain	• Dominance		• Organizational Gain	• Personal Financial Gain • Coercion
Sensationalist	• Notoriety			• Notoriety	
Terrorist	• Ideology	• Disgruntlement	• Dominance • Organizational Gain	• Ideology	• Ideology
Thief	• Personal Financial Gain			• Personal Financial Gain	• Personal Financial Gain • Personal Satisfaction
Vendor	• Organizational Gain			• Organizational Gain	• Personal Financial Gain

For more information on Intel security practices, visit www.intelsecurity.com.


¹⁴ Intel white paper, September 2007. "Threat Agent Library Helps Identify Information Security Risks."

² IT@Intel white paper, December 2009. "Prioritizing Information Security Risks with Threat Agent Risk Assessment."

³ D. Cappelli, A. Moore, R. Trzeciak, and T. Shimeall, 2009. "Common Sense Guide to Prevention and Detection of Insider Threats" (3rd Edition). CERT/Software Engineering Institute.

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

Copyright © 2015 Intel Corporation. All rights reserved. Intel and the Intel logo are trademarks of Intel Corporation in the U.S. and other countries.

*Other names and brands may be claimed as the property of others. Printed in USA 0215/TCAS/KC/PDF  Please Recycle

