




Ethical competitive intelligence in software

HOW TO LOWER YOUR RISK, IMPROVE YOUR RESULTS AND AVOID BEING PART OF AN INDUSTRY-WIDE PROBLEM

WHY YOU NEED TO CARE ABOUT COMPETITIVE INTELLIGENCE



Competitive intelligence (CI) research can put your software company in a strong position to create licensing, packaging and pricing strategies that give you an advantage. But if done unethically, it becomes corporate espionage. As such, it could expose you to risks of legal, operational and reputational damage. Not only that, but you could also risk making poor decisions from inaccurate information.

WHY YOU NEED TO CARE ABOUT COMPETITIVE INTELLIGENCE



When conducting CI, many software executives are unaware of how exposed they are to risk. Just like software pricing, CI is a systematic, highly skilled professional discipline. So, if you're assigning employees-whose main competencies are something else-to do a little intelligence gathering on the side, you could be heading into deep water. You could end up on the same slippery slope by hiring pricing consultants who fold intelligence gathering into their engagement, even though CI is not their area of expertise.

On the flip side, many software executives are unprepared for unethical CI conducted on them. They don't know their rights or what to do when something suspicious occurs. They're not taking the necessary proactive measures to protect their company's trade secrets and other confidential and proprietary information.

In this ebook, we hope to provide practical guidance on how to avoid becoming a perpetrator or victim of corporate espionage. We also want to address the danger these unethical practices pose for the software industry, where the risk of fraudulent behavior being elevated to the level of industry normalcy is growing.

It is time to be clear and straightforward about what is right and what is wrong about competitive intelligence in the software industry. Here are the things you need to know and what you can do to keep your company on safe ground.

One small step after another...until Most companies do not intentionally commit corporate espionage, at least not at first. They just take one small step away from the ethical shoreline, then another, which leads to another. At some point, glancing back, there's the shocking realization of the distance between them and the shoreline. The rest of the business community, on shore looking out at them, is thinking, "How did they allow themselves to go so far?"

So, don't take the first step.

Stay on safe ground

Page Know your risk

- 3 Know your risk when conducting competitive intelligence (CI)
- 3 What is unethical CI?
- 3 The CI risk-reward spectrum
- 4 Top three risks from unethical CI
- 6 Examples of legal action against companies that went too far
- 7 Third-party provider warning signs
- 8 Is "We didn't know" a valid excuse?

Know your rights

- 9 Theft of trade secrets
- 9 Unfair competition
- 9 Other unethical tactics
- 10 Top six counterintelligence best practices
- 11 Telltale signs you're being mystery shopped

Why ethical CI works better

- 12 What is ethical CI?
- 12 Accurate and reliable insight
- 13 Built on repeatable truth

The future

- 14 The future of competitive intelligence in the software industry.
-

KNOW YOUR RISK

Know your risk when conducting competitive intelligence

Software companies that conduct unethical CI, or engage a third-party that acts unethically, do their organizations more harm than good. For one thing, they're likely to be on the receiving end of intensely combative, determined actions by the victimized competitor, as the information obtained unfairly is right at the heart of the company's revenue model—how they deliver value and make money.

People get emotional about that. They feel a basic sense of fairness has been violated. This feeling can activate a defense mechanism that puts the opponent into fight mode. Among the many cases we've witnessed is one where a board member of an entrepreneurial company became so incensed, he personally funded the entire lawsuit. Be careful what you unleash.

DRAWING THE LINE ON ETHICS: THE CI RISK/REWARD SPECTRUM.

**ETHICAL
COMPETITIVE
INTELLIGENCE**

**UNETHICAL
COMPETITIVE
INTELLIGENCE**

What is unethical CI?

Unethical CI is the use of intelligence gathering methods that misrepresent who you are and the purpose of an interaction. For example, it would be unethical to call a salesperson at a competitor and try to get information about their volume discounting and net prices by pretending to be a prospective buyer. It would also be unethical to hire a former employee of a competitor and get them to violate their nondisclosure agreement by divulging proprietary and confidential information, as was recently publicized in a significant court case adjudicated in May of 2022 (see "Pegasystems" on page 6 for details).

Rewards

↑
Deeper competitive insights, accurate and detailed information for decision making, reputational integrity, operational transparency and simplicity. A valuable, incrementally expanding organizational knowledge base.

Risks

↓
Lawsuits, distractions, lost time, legal fees, court costs, fines, reputational damage, inaccurate information for making decisions.

Top three risks from conducting unethical competitive intelligence:

1. You get sued

While it's possible you might not get caught using unfair, deceptive methods, if you are, there's a very high probability you will be sued. The odds of legal action go up because of the emotion previously cited. Another reason is purely pragmatic. Victimized companies think: "If I let this stand, you're going to do it again, or others will. Who else is going to take advantage of me if I don't fight back?"

Lawsuits are expensive. Even if you're able to get the suit dismissed, the legal fees would likely run into six figures. If you go to trial and lose, your legal bill will multiply many times over, and you'll have to cover court costs and the plaintiff's legal expenses too. In addition, many plaintiffs will try to extract damages, out of a sense of both principle and punishment. If you're found guilty of unfair and deceptive practices, treble damages could apply. Case in point: in 2022, a jury imposed a \$2+ Billion judgment in a case involving two software competitors (see "Pegasystems" on page 6 for details).

2. You get distracted and slowed down

Even if you win the case, you'll lose organizational focus and speed. Your CEO and other execs will be spending time with your legal team working on discovery and defense strategies—time that could otherwise be spent developing better licensing, packaging and pricing strategies.

Think this through especially if you're a fast-growing, disruptive competitor using unethical CI against a large incumbent. They've got the staff and budgets to take extended legal action without blinking. What could be better for them than a multi-million dollar lawsuit to slow you down enough to close the gap between their product line and yours?

3. You get a bad reputation

No matter the outcome of the case, your company is likely to incur reputational damage. Even if a suit is never brought, your unethical behavior can carry consequences. With the porous movement of people through the software industry, a bad reputation is almost impossible to contain and control. That's a big risk at a time when corporate ethics are weighing heavily in the decisions people make about buying from or working for a particular company.

Expect companies that feel victimized to do everything they can to spread the word about your unethical tactics and whip up outrage. If what they're saying is factual—especially, of course, if their claims are supported by a legal judgment—there may not be much you can do to contain the reputational damage.

Do your customers and employees care about your ethics?

Increasingly, the answer is yes, especially when it comes to younger generations.

Research by Deloitte found that over a third of consumers in 2020 “value ethical practices in the products and services they buy”—with Gen Z valuing ethics the most. A January 2021 study by the Bauer Leadership Center at Washington University in St. Louis and Vrity, a brand measurement company, found that 55% of US consumers surveyed said they were paying more attention to brand values than a year ago.

55%

of US consumers are paying more attention to brand values than a year ago.

Red-faced on the cover of... everywhere

Way back in the '90s, a leading pharma/personal care company found itself exposed and embarrassed on the covers of the Wall Street Journal and Washington Post. The company, which had engaged in perfectly ethical CI practices, was accused of not following its own code of ethics, which expressly prohibited any such activity.



What happened to this company seems unfair (especially since insiders suspect the press obtained the scoop from the company's main competitor, which was in fact engaged in illegal CI, including stealing laptops from its rival's employees). Even so, there's a lesson to be learned: Check your company's code of ethics before you hire a contractor or adopt a CI approach.

It's even more important these days to act in an above-board manner. Unlike the '90s, it's not just ending up on the cover of newspapers you have to worry about. There are now so many more types of publications and other channels for holding organizations accountable.

As Enza Iannopollo, Principal Analyst at Forrester warned in October 2020:

“Technology—from social media to public employee platforms to supply chain monitoring software—is exposing your business processes. This is a critical change. Customers can see, employees can say, and business partners can easily demonstrate whether a company is behaving accordingly with the values it publicly marries. Values-based customers and employees act on the basis of what they learn.”

KNOW YOUR RISK

Legal actions against companies that went too far

Company	Pegasystems	Mattel	Fujitsu	DGI Technologies
Legal Action	<p>Pegasystems was sued by Appian for trade secret misappropriation in Fairfax County, Virginia.</p> <p>Appian Corp. v. Pegasystems Inc. & Youyong Zou; Civil Action No. 19-11461-PBS filed May 29, 2020 in state court in Virginia.</p>	<p>Mattel was sued by MGA for trade secret misappropriation under California state law.</p> <p>Mattel, Inc. v. MGA Entm't, Inc., Case No. CV 04-9049 DOC (RNBx) (C.D. Cal., filed Nov. 2, 2004)</p>	<p>Fujitsu was counter-sued by Tellabs for misappropriation of trade secrets under Texas state law. This case happened prior to the Defend Trade Secrets Act of 2016. If it happened today, the parties could sue under both federal and state law (though they cannot double-recover).</p> <p>Fujitsu Ltd. v. Tellabs Operations, Inc., Case No. 12 C 3229 (N.D. IL, filed Apr. 30, 2012)</p>	<p>DGI Technologies was sued by Alcatel for trade secret misappropriation, unfair competition and tortious interference under Texas state law. DGI was also sued for copyright misappropriation.</p> <p>Alcatel USA, Inc. v. DGI Techs., Inc., Case No. 97-11339 (5th Cir., decided Jan. 29, 1999)</p>
Outcome	<p>Appian won a jury verdict for trade secret misappropriation. The jury also found that Pegasystems violated the Virginia Computer Crimes Act and found Pegasystems' misappropriation of Appian's trade secrets to be willful and malicious.</p>	<p>Found guilty of willful and malicious conduct that "fell far short of basic ethical standards."</p>	<p>Tellabs won against Fujitsu's motion to dismiss the trade secret misappropriation claim after the court found Tellabs had adequately pled that Fujitsu engaged in "improper means of acquiring Tellabs' trade secrets."</p>	<p>Trial court found that DGI was guilty of trade secret misappropriation and unfair competition.</p>
Costs	<p>The jury awarded Appian \$2.036 billion in damages from Pegasystems., with the possibility of additional award of attorney's fees.</p>	<p>Court granted MGA exemplary damages of \$85M, \$2.172M in attorney's fees, and \$350,000 in costs.</p>	<p>The case went on for nearly two years before settling for an undisclosed amount.</p> <p>Total costs, including ongoing litigation over the two years, are unknown.</p>	<p>Court awarded \$4.3M in actual damages and \$7M in punitive damages. Later, the appellate court agreed that DGI had acted wrongly but remanded the case for a new damages calculation because the state law claims were preempted by the federal copyright claim brought in the case.</p>
Details	<p>Pegasystems hired a third-party contractor (who worked as a developer for Appian under a government contract) for the purpose of getting him to violate his employer's code of conduct and agreement with Appian by disclosing proprietary intellectual property, including trade secrets. It was further shown that Pegasystems employees—including the company CEO—had used false identities, and made up fake personas and companies, to obtain access to Appian information.</p>	<p>Such conduct included years of senior management encouraging employees to use false pretenses (fake business cards, nicknames, etc.) to access competitor's private displays at international toy fairs and improperly acquiring competitive information, including price lists, advertising plans and unreleased product attributes, and then disseminating such wrongfully acquired information for monetary gain.</p>	<p>Fujitsu allegedly obtained manuals and software "through means that were not 'fair and honest'": (1) unauthorized copy of a presentation marked as "not for use or disclosure outside the [Tellabs' companies] except under written agreement," and the allegedly disclosing company's employees were subject to confidentiality obligations; and (2) Tellabs' equipment manuals and software from an unrelated eBay vendor, taking specific measures to hide Fujitsu's identities from the eBay seller and falsely representing that the purchasers were acting on behalf of another entity.</p>	<p>Evidence showed that the Defendant unlawfully made a copy of Plaintiff's operating system software by misleading an employee of one of Plaintiff's customers, and that Defendant then used the information obtained to interpret the trade secrets contained in Plaintiff's firmware. The Court held that a reasonable jury could have found that such means "[fell] below the generally accepted standards of commercial morality and reasonable conduct," and thus were obtained through improper means.</p>

These are just a few examples. There are dozens of other, similar cases.



Third-party provider warning signs

Sometimes, software companies hire consulting firms to do competitive intelligence without asking enough questions. Because ignorance is not a defense where illegal activity is involved (See page 8, **Is "We didn't know" a valid excuse?**), you should ask consultants to describe their work process in detail. If they're not fully transparent, that's a danger sign.

Other signs can be found in the amount of time they need to complete the assignment and how much they're going to charge. If you're being promised the world in a couple of weeks, look closer. Some firms have a revenue model that depends on factory-like production of competitive reports. The only way they can keep the pace is to deliver weak reports or employ shady methods.

Ask the consultant for information about the backgrounds of the people who will be doing the CI work. How much training and experience in CI do they have? Are they certified by the association of Strategic and Competitive Intelligence Professionals (SCIP), whose code of ethics explicitly requires "accurately disclosing all relevant information, including one's identity and organization, prior to interviews"? Competitive intelligence is its own specialized field of expertise, and to avoid problems, you should expect highly trained CI professionals to do the work.

When is mystery shopping OK?

There's nothing wrong with mystery shopping as it has been practiced since the mid-20th Century by the hospitality and retail industries. Typically, mystery shopping is conducted within one's own organization to evaluate employee performance and adherence to corporate policies and standards. In recent decades, it has also been used to better understand and improve customer experience.

While it's true that this technique involves misrepresentation of who the shopper is and why they've initiated the interaction, the purpose of this misrepresentation isn't nefarious. The mystery shopper is after information that the company has every right to acquire.

This veered into unethical territory for the software industry when companies started using mystery shopping techniques against competitors to try to trick them into divulging proprietary and confidential information. Posing as buyers, they call competitors' salespeople and customers. That's misrepresentation of the worst sort. Calling it "mystery shopping" is co-opting an acceptable practice—with terminology that sounds fun and friendly—for unscrupulous purposes.

Is “We didn’t know” a valid excuse?

Could your company be held liable for the activities of a third party acting on your behalf? There is some precedent to think so when you look at legal and regulatory actions over the past decade.

For instance, the US Consumer Financial Protection Bureau (CFPB) has put financial institutions on notice that they “may be held responsible for the actions of the companies with which they contract.” So, if a bank contracts an agency to collect debt on its behalf and that agency violates the Fair Debt Collection Practices Act (FDCPA), the bank could be fined by the Bureau or sued by the victim.

Along the same lines, in another area of federal regulation, Dish Network incurred a \$61 million judgment in a class action suit for “repeatedly looking the other way” as a third party it had contracted committed many violations of the Telephone Consumer Protection Act (TCPA). In this 2017 ruling, the judge tripled the jury’s finding of \$20.5 million in statutory damages, saying that Dish should have known what the third party was doing, and so was itself guilty of a knowing and willful violation of the TCPA. The judgment was upheld in 2019 by the Fourth Circuit Court of Appeals.

Theft of business trade secrets is not governed by this sort of federal regulation, but rather by tort law. A tort, in common law jurisdiction, is a civil wrong that causes a claimant to suffer loss or harm, resulting in legal liability for the person who commits the tortious act. Tort law includes claims involving harm caused by a wrongful act such as negligence, financial losses, injuries, invasion of privacy, misappropriation and more.

In general, tort law does not hold a principle liable for the actions of an independent contractor. But there are two exceptions:

- 1) when the work is inherently dangerous;
- 2) when the work is illegal.

There is nothing to prevent a competitor from bringing suit against both contractor and principle. The court could find your organization negligent, which is generally defined as a failure to behave with the level of care that someone of ordinary prudence would have exercised under the same circumstances.

While commercial liability insurance generally covers negligence, it doesn’t usually extend so far as fraud. So, if your competitor is able to convince the jury that the contractor’s activities were illegal—and you knew that—your company might not have coverage.

How likely is it that a jury would come to such a decision? Perhaps more likely than you might think. Unethical behavior sits in the area of right and wrong, and most people—including jurors—know the difference. For this reason, the company suing may like their odds of winning and receiving a substantial award for damages as well as permanent compensatory injunctions. So they’re incentivized to go the distance in a trial—especially when triple damages are up for grabs.



Know your rights when competitive intelligence is conducted on you

Software companies do not have to put up with the growing incidence of corporate espionage. There are plenty of things you can do to protect your organization's secrets. Here are some of the laws, regulations and best practices you need to know about.

Theft of trade secrets

Like any other business, software companies have the right and obligation to defend their trade secrets.

A trade secret, according to the US Patent and Trademark Office, meets these three criteria:

1. Is information that has either actual or potential independent economic value by virtue of not being generally known
2. Has value to others who cannot legitimately obtain the information
3. Is subject to reasonable efforts to maintain its secrecy

Unlike a patent, which has an expiration date, trade secrets are protected *ad infinitum*, if they continue to meet all three criteria.

The case examples presented earlier were all brought at a time when only state law claims existed to protect trade secrets in a civil case. The Defend Trade Secrets Act (DTSA) was added in 2016 as a federal-level civil remedy. It provides a consistent way of protecting trade secrets anywhere in the country. You can still resort to state laws if you like, but you have the choice of pursuing legal remedies in a federal venue. If you decide to go the state route, realize that while most states have aligned their laws with the legal framework of the Uniform Trade Secrets Act (1979; 1985), some have modified versions of the statute—kind of like a Microsoft or Apple version of an industry technology standard.

Theft of trade secrets may also be criminal. Prior to the 2016 passage of the DTSA, trade secret misappropriation cases were always considered criminal in nature. In that context, the US Economic Espionage Act (1996) covers trade secret

thefts benefiting foreign governments and entities. It also covers thefts “related to a product or service used in or intended for use in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will injure any owner of that trade secret.” Both types of offenses are prosecuted by the US Department of Justice and are punishable by imprisonment and/or fines. If your case is eligible—separate from any civil action you might bring—you can submit it to the Justice department, and they may take it on. To do this, contact your local US Attorney's Office.

Note: You can't sue for both trade secret misappropriation and copyright infringement for the same bad act. To bring both claims in a single lawsuit, you have to be able to prove separate bad acts for each.

Unfair competition

State common law (derived from judicial decisions rather than statutes) protects business information that does not rise to the level of trade secrets but is still obtained and/or used in an unfair and deceptive way. Some states have also codified common law rules into statutes. For instance, the California Unfair Competition Law covers unlawful, unfair or fraudulent business acts or practices, where the victim can prove resulting suffering and financial or property losses.

The Federal Trade Commission (FTC), which mainly aims to protect consumers from deceptive trade practices, also provides some remedies for competing businesses injured by such practices.

Other unethical practices

Depending on the type of behavior involved, tort laws in some states may provide other avenues for protection and remediation. In addition, perpetrators of unethical CI could be liable for fraudulent misrepresentation under state contract laws if it's proven they knowingly made misrepresentations to another party who relied on these misrepresentations and suffered harm as a result. Contract law provisions might also apply if fraudulent misrepresentation induced a competitor's employee, former employee or customer to breach a nondisclosure agreement.



Top six counterintelligence best practices

The first step in defending your proprietary information is to prepare as if it is inevitable that, sooner or later, somebody is going to come after it in an unethical way. Think of these counterintelligence best practices as your security system:

- 1. Clearly mark private information.** Make sure all written information your organization considers proprietary and confidential is conspicuously labeled as such. Oral information, such as your talk-through when giving a detailed presentation to a sales prospect, should also be identified as proprietary and confidential. You can do this verbally before you start talking. Even better: As part of your preparation for the meeting, state in an email that what you'll be sharing—both in slides and orally—is proprietary and confidential, then confirm this after the meeting in your follow-up email. All emails should also have proprietary and confidential footers.
- 2. Copyright product and sales documents.** Even though some of this information may be available on your public website, and thus is not confidential, it is proprietary. Copyrighting it provides all users with forewarning that your company intends to protect its IP. While taking this measure probably won't provide strong grounds to argue unfair competition, it is another layer in your defense. Say a competitor takes your copyrighted information and disseminates and/or uses it improperly. Copyright gives you another avenue to pursue, which, at minimum, will wrap your competitors up in litigation for a while.
- 3. Use NDAs and mutual NDAs.** Most software companies already use nondisclosure agreements for employees and independent contractors. Make sure these are fully signed before you start projects. In some cases, depending on the conversations you need to have as part of the hiring or contracting process, you may want to execute an NDA before bringing the employee or contractor on board. When working with service providers, mutual NDAs are common and readily available.
- 4. Obtain written assurances before engaging in potentially revealing conversations.** Even in preliminary discussions with a prospect, think about the nature of the information you might share through phone conversations, emails and other interactions. If there's a possibility of revealing private information, make sure to include a written notice of confidentiality in your emails (something beyond the standard footers). You can also ask the other party to send you a simple email stating the purpose of their inquiry and including a representation that they will not share the information with your competitors or a third-party research firm. On the phone (in states where it's legal to record conversations with permission of the other party), you can state the confidentiality notice and obtain a verbal assurance at the beginning of your talk.

Some software companies also require customers, and even fully qualified leads that have reached the comparative research or negotiation stages of the sales funnel to sign NDAs. It is true that asking prospects to sign an NDA introduces an extra step in the sales process, which may not be something you want to do. And it may not be feasible for high-volume business models offering point solutions. But for complicated enterprise offerings, a mutual NDA is something to seriously consider. The benefit is that more serious buyers will sign—which not only further qualifies them, but also immediately increases the value of what you, the seller, are offering. It's not just software anymore—it's your intellectual property. The NDA also communicates to the buyer that there is an obligation here. And if you are talking with a mystery shopper, who gets caught, and you sue, the NDA is the first link in a powerful chain of events that will help as you go through discovery.



5. Train your sales force (first) and other employees (next) in counterintelligence procedures. Set out clear procedural guidelines covering #s 1,2,3 on the previous page, and train your people to adhere to them. Start with the sales force; they're the most common target of unethical CI. Do it from their first day on the job, since the least experienced salespeople are often the most easily duped by mystery shoppers deployed by competitors or their agents. They tend to immediately spin into sales mode without asking the questions they should ask first. Give them the information and mentoring they need to reliably

detect and deflect these acts of corporate espionage. See below **Telltale signs you're being mystery shopped.**)

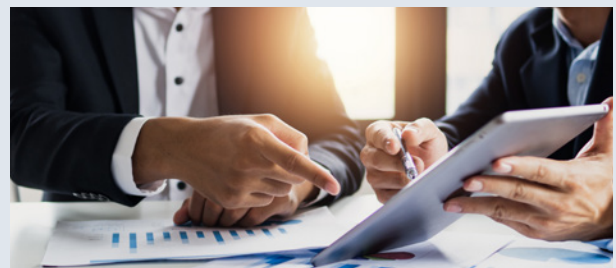
6. Work with your legal team on proactive strategies and contact them immediately when something suspicious happens. Don't wait until you've been fooled before examining your legal options. Ask your lawyers to help you put defensive measures in place ahead of an espionage event. Also have your plan for what to do when it happens locked and loaded so you can act swiftly and efficiently.

Telltale signs you're being mystery shopped

Experienced software salespeople and executives often say they can sniff out mystery shoppers pretty quickly. Here are some of the things that set their noses twitching:

- **The lead comes in under the radar.** A lot of these interactions somehow become sales-qualified leads without first being marketing-qualified leads or otherwise making their way through the normal sales funnel. Pay attention to sales opportunities that emerge in unusual ways.
- **The buyer's story is weak.** Because mystery shoppers are fabricating their identities and reasons for contacting you, their stories are often weak and lacking depth. Asking questions, you'll often find these buyers evasive. When they do try to answer, the details of their organization, job responsibilities and use case just don't line up. And even though business spies may set up fake profiles on LinkedIn, Facebook and other social media, a little web-savvy research will usually reveal inconsistencies (or too much consistency across the supposed employees of a supposed company) to confirm your suspicions that the sales opportunity isn't real.

- **The buyer asks a lot of questions outside of their original story and use case.** While mystery shoppers don't like to answer your questions, they sure like to ask questions of you. These will often veer outside of the scenario for which the conversation was initiated. Business spies tend to quickly start asking wide-ranging questions you wouldn't expect from a real buyer, or at least not so early in the discussion. They might ask about your pricing model generally, as opposed to what price you could give them for a specific number of licenses. Or they might throw out lots of hypotheticals. Maybe they started out saying they needed ten licenses, but suddenly they're blue-skying: "What if my company grows to 200 users? How about 500?" They might ask you to tell them what use cases you're seeing with other companies in "their industry." They might probe for details of your product roadmap.



WHY ETHICAL CI WORKS BETTER

Wouldn't it be great if there were a way to gather the competitive insight you need to manage your business, but not carry the risks or the stench of unethical CI? There is. And it is time for the software industry to take it seriously.

What is ethical CI?

Ethical CI is the use of intelligence gathering methods that are trustworthy. For instance, when an ethical CI specialist contacts a competitor's customer or former employee, they clearly state who they are and the purpose of their inquiry. If they learn that the individual is under NDA, they do not encourage them to breach their obligation, but terminate contact.

This approach works because the foundation of transparency makes it possible to engage knowledgeable people in real conversations. In this way, ethical CI is really an extension of your customer research. You are learning how even your competitors' customers, not just your own, think about the category, the critical capabilities they need and opportunities to offer more valuable capabilities in your roadmap.

Accurate and reliable insight

Of utmost importance, ethical CI also yields more accurate and reliable insight. Because unethical mystery shoppers usually try to extract information from novice salespeople with less experience to know they're being duped, they usually get a sales speech, list prices, inaccurate net prices and the salesperson's interpretation of what customers care about. Such findings can be misleading because the salesperson's interpretation may not reflect the reality of what's really going on with the competitor's products, pricing model and customer relationships.

Another reason such findings aren't accurate is that the process is unnaturally rushed. Unlike real customers, mystery shoppers aren't having multiple discussions with salespeople over weeks of dragging their feet and wrangling for a better deal. They're not arguing that a partial use case for a one-size-fits-all product should entitle them to a discount. The deal being negotiated isn't making its way up and down the

sales chain of command for iterative modifications and approval.

Too often, software companies take these mystery shopping findings at face value and use them to either copy what they believe is their competitor's pricing model or set their own price points in relation to it.

This means some companies are building their strategy on inputs from people fresh out of college, discounting like crazy because they aren't experienced enough to know how to communicate and sell value.

In contrast, ethical CI practitioners take the time and do the hard work to seek out and have real conversations with competitors' customers. They go beyond low-hanging fruit to discover more valuable insights about their rivals, such as accurate net prices, details about licensing metrics and the structure of packaging, terms and pricing. They find out if the competitor has a structured, disciplined approach to volume and competitive discounting or not. Through extended conversations, they gradually learn the details of customers' use cases and particular requirements, what parts of the sales pitch resonated with them, what they value that ultimately led them to buy and their real-world experience during the sales and negotiation processes, as well as pre-and post-implementation.

The reward for not taking shortcuts is richer insights. For example, suppose a competitor offers a 24-hour hotline—wouldn't it be interesting to find out how long it takes them to answer a call or email, and also their actual time to resolution? Maybe you discover that your competitor often fails to respond to customer inquiries because it is understaffed.

Here's a pretty dramatic real-world case in point: During a recent CI project, it was discovered that a competitor's artificial intelligence engine was actually an overseas team performing manual translation of audio recordings. This discovery enabled the sales team to easily debunk the competitor's claim of feature parity, and it also provided an important insight for value-based pricing.

WHY ETHICAL CI WORKS BETTER



Patience, persistence and creativity—that's how ethical CI experts piece together the complex mosaic of what really happens when your competitor's products and list prices hit the street. That's the kind of truth you want to build your strategy on.

Repeatable, transparent truth

Once presented in a PowerPoint deck, findings from unethical CI take on a life of their own. Inaccurate information ends up being used as factual input to all kinds of important decisions, generally mucking things up in a way that makes it difficult to understand what exactly went wrong. The result is confusion, complexity and unnecessary cost.

Ethical CI is rooted in reality. You will always be able to trace it back, to explain and justify the competitive intelligence you are basing decisions on. It is simpler to understand how the information is influencing various parts of your operations and direct its use appropriately. You can also build on ethically gathered competitive intelligence in a modular, incremental way, not unlike building software components and layers.

You can reliably connect insights from different projects to form a valuable knowledge base and accurate model of how your markets work and are changing. Over time this becomes a powerful source of competitive advantage and, in and of itself, part of your organization's unique IP.

THE FUTURE



The future of competitive intelligence in the software industry

The big-picture issue with unethical CI goes beyond its effect on an individual software company's operation, extending to its impact on the larger business environment in which we all operate. When companies and consultants participate in unethical CI, they contribute to such behavior becoming institutionalized throughout the industry, a situation that in the long-term would be extremely costly and self-limiting.

It is not hard to envision how this has already begun to happen: Employees of one company get the idea they're being encouraged to take shortcuts. It seems okay to take a step or two away from the ethical shoreline, and then a step or two more. Then they jump to another company, maybe even the victimized competitor, and bring that attitude with them.

Sooner or later the general lack of transparency and trust in the environment, the expectation that you have to game the system because everyone else is doing it, affects all participants. This leads to a pervasive distrust in pricing integrity that has buyers spending unnecessary time, effort and money issuing RFPs, software providers jumping through hoops responding to them, and buying decisions pushed to the last minute of the seller's fiscal year to force discounts.

Competitive intelligence is an important and valuable element of business and pricing strategy. But it can only deliver true and applicable insight if software companies properly evaluate CI providers and protect themselves from unethical CI attacks.