Countering Your Competitor's CI

Ten tips from FreshMinds

Here are some guidelines on how companies can protect themselves against ethical CI inquiries and the occasional unethical rogue practitioner. As your company tries to gain intelligence on others, you can leave yourselves vulnerable to the same kind of probing.

1. Good gatekeepers

As the first port of call for enquiries is usually the switchboard – company switchboard numbers are available online or via directories – it is there that 'gatekeepers' are most commonly located. Almost all large companies recognize the value of good gatekeepers: people tasked with keeping out all inquirers not necessary to the functioning of the business. Most switchboards have a simple but effective gate keeping policy – only let calls with named contacts through.

On top of the basic policy, gatekeepers need to be aware of competitive intelligence techniques to screen calls effectively. The CI professional has several methods to cross this first line of defence. At a minimum, it can be surprisingly easy to pass the gatekeeper by conveying a sense of legitimacy: speaking authoritatively and suggesting a job title – "Please put me through to the Head of Marketing" – is frequently effective. A second tactic is to ask obliquely for contact information, phrasing the inquiry as a request for information rather than for access: "Could you confirm to me that the Head of Marketing is Christopher Jones?" Gatekeepers tend either to confirm the name or to correct it: the CI professional can then be put through later as a legitimate caller.

Finally, policies and awareness-raising have to be extended to all interfaces with the public. Although most companies have a switchboard gatekeeping policy, other access points are less well protected. Departments like Investor Relations, Human Resources or Help Desk – whose numbers are also readily available - are public-facing and their staff are trained and encouraged to be helpful to incoming calls. It is all too easy for the competitor intelligence professional to ask these departments for contact names and numbers, and even a description of organizational structure. Companies need to be aware that these outward-facing departments will be approached and that these staff should be trained in security awareness.

2. Strengthen non-core offices

Companies should not fall into the trap of assuming that their headquarters is the only point of access. Regional and satellite offices offer oblique access points to the CI professional, and in our experience regional offices, support staff and distributors are often overlooked by and isolated from headquarters, resulting in much lower security awareness.

Satellite offices or facilities staff can be very willing to discuss their company's structure, product, and employee numbers. Regional staff need to be aware of security policies and implement those policies consistently across all locations.

3. PR support

Public relations departments are companies' main interface with the outside world, and their staff are well-attuned to the tell-tale signs of probing from journalists, researchers, and competitor intelligence professionals alike. Gatekeepers and employees should consider diverting all research-related enquiries to the PR department, who may be best placed to judge whether the request is likely to be legitimate or not and formulate an appropriate response.

4. Hard copy

It may also be advisable to insist that all enquires are made in writing, either by email or in hard copy. Written requests help employees to either clear requests with their managers before responding, or to pass requests on to the PR department. CI professionals are frequently disappointed when companies insist on written requests, as it robs the CI professional of their fastest and most effective tool: the telephone.

5. Stalling

While stalling is generally considered unprofessional in most business environments, if research is often done under tight deadlines. Stalling may persuade the researcher to look elsewhere for information. As a general rule, however, if you are unwilling to respond to any part of the query it is best just to say so.

6. Hard line policies

Controlling the point of contact is just the first line of defence in what should be a detailed and widely disseminated CI protection strategy. Companies should determine what information is commercially sensitive, and should periodically review its classifications. These classifications should then be communicated to staff at all levels and all locations.

This hard second line of defence can be reinforced by making the dissemination of sensitive information to external contacts a disciplinary offence. For this to be enforceable, staff will need to be frequently updated on information classifications and induction programs developed to ensure junior and new staff are resistant to external probing.

It may also be necessary to remind staff that these hard line policies must also be enforced outside the office. As in any other social context, employees may find that they let their guard down at conferences and networking events, and hence be more vulnerable to probing questions. This is also the case of sales meetings or meetings with service providers or distributors, who may themselves be targeted by competitor intelligence professionals as potential sources of information. When it is necessary to reveal commercially sensitive information it is often prudent to ensure that it is protected by a non-disclosure agreement.

7. Need to know policies

The logical complement to a hard line security policy is to ensure that sensitive information is only disseminated on a need-to-know basis. 'Chinese Walls,' more commonly associated with preventing conflicts of interest, can be particularly useful for the task. By ensuring employees only have access to information that they need to perform their specific roles, they reduce the risk that sensitive information could leak out obliquely.

Robust internal PC security is vital to the effectiveness of such a strategy, as is the routine shredding of sensitive documents. A carefully enforced information policy will give your employees the strongest defence against CI enquiries: employees can honestly claim that they do not hold any information on anything outside their narrow field.

8. Controlling the internet

Companies maintain an internet presence for the public and for investors. Although I would usually caution companies to put the bare minimum of information into the public domain, there are some advantages to a carefully crafted information-rich website. If the information is properly screened, companies can refer all research inquiries to the website with the statement that all public domain information can be found there.

Employees should be made aware of what information is available on the corporate website, and it should be stressed that no other information should be given out to third parties without managerial authorization.

The explosion of online forums and blogs poses tricky questions for companies. Blogs and forums are strikingly effective communications media, but employees may be unaware of the fine line between maintaining good public relations and leaking commercially sensitive information. Companies should consider employee participation in blogs and forums on a case-by-case basis, but content should be carefully monitored or even written by senior staff to ensure that sensitive information is not divulged.

In isolated cases, however, disgruntled employees may intentionally divulge sensitive information, as epitomized in the infamous website www.internalmemos.com. Companies operating a need-to-know policy will be shielded from the full risks of such action, but it may be worth bearing the possibility of leakage in mind when publishing information internally.

9. Public records

All companies must meet certain statutory disclosure requirements. These requirements are designed to ensure that a minimum of information is available to the public. Any disclosure of information beyond that minimum – particularly information aimed at investors – should be evaluated on a case-by-case basis in terms of how commercially sensitive the information may be and whether the benefits of explanation outweigh the risks of disclosure.

Companies should also be careful about the information disclosed if they submit themselves for business awards and should brief spokespeople who communicate with analysts or journalists. Remember: there's no such thing as 'off the record'!

10. Physical security

Companies may find retail outlets used for benchmarking research – for instance, price comparisons – or store layout research. Security and floor staff need to be briefed on what such research looks like so that they can spot researchers.

While no SCIP member would go through a target company's garbage, it is good practice to be protected against unethical practitioners or competitors by making sure that buildings are secure. All sensitive documents, disks, and internal memos should be disposed of by a sensitive documents recycler or shredded.

In summary
The tension between CI professionals and companies on the receiving end of their enquiries is entirely natural. Protecting a company from investigation is a significant investment in time and energy, while CI professionals are both dedicated and ingenious in their pursuit of information.

But the reality is that few companies would pass up the opportunity to learn what their peers are doing: intelligence gathering is just another facet of the vibrant competition that marks a healthy economic system. And CI professionals are just that: professionals. FreshMinds, like other SCIP members, identify itself and its research honestly, allowing a target company to refuse to contribute.

Nevertheless, some rogue players don't play by the rules. Be warned.

About the author

FreshMinds www.freshminds.co.uk is a business research consultancy. As part of strategy reviews, new product development and new market entry strategies, FreshMinds conducts ethical primary and secondary research on clients' competitors. Claudia Brendel, the author of this piece, runs the FreshMinds Competitor Intelligence practice.

Please email her on claudia.brendel@freshminds.co.uk
Or call FreshMinds on +44 (0)870 9037374