INTELLIGENCE · ORGANISATIONAL INTELLIGENCE

"Counterintelligence for Businesses: Protecting Against Espionage"

Businesses gather intelligence about their competitors, and competitors, criminals and some states gather intelligence about them. This article explains counterintelligence in a business setting: how commercial information is targeted, the line between legitimate competitive intelligence and espionage, the role of insiders, and how to build a practical programme to protect what matters most.

ModQu research article · 2,889 words · 24 references (APA 7th edition)

Every organisation that gathers intelligence about its competitors should assume that its competitors are doing the same. Most of this activity is legal and ethical: reading published reports, attending trade fairs, talking to customers, analysing patents. Some of it is not. Trade secrets are stolen by departing employees, confidential plans are obtained through deception, systems are penetrated by criminals and state-sponsored groups, and sensitive information leaks through careless conversation. **Counterintelligence** is the set of activities that protect an organisation against such efforts. In government, it is a long-established discipline. In business, it is often neglected until a loss occurs.

What counterintelligence is

Prunckun (2019) defines counterintelligence as the activities undertaken to protect an organisation's secrets and operations from the intelligence efforts of opponents. It has two broad aspects. **Defensive** counterintelligence denies opponents access to information, through security measures, awareness and procedures. **Offensive** counterintelligence detects, investigates and disrupts opponents' collection efforts. Herman (1996), in a study of intelligence in government, describes counterintelligence and security as the protective side of intelligence, concerned not with what an organisation can learn about others but with what others can learn about it.

In a business setting, offensive measures are limited by law and ethics. Businesses cannot run surveillance operations against competitors or feed them deliberately false information in ways that cross into fraud. Business counterintelligence is therefore mostly defensive: understanding what information is valuable, who might want it, how they might try to get it, and how to stop them or detect them if they try.

The threat to business information

Economic espionage

Nasheri (2005) documents the scale and methods of **economic espionage** and industrial spying, showing that commercial information is targeted by competitors, criminals and foreign governments seeking economic advantage. The American National Counterintelligence and Security Center (2018) reported that foreign intelligence services and their proxies use cyber operations, insiders, joint ventures, academic collaborations and investment to acquire technology and business information from American companies, and that small and medium-sized firms, which often have weaker defences, are targeted alongside large ones.

A widely cited example is Mandiant's (2013) report on a hacking group linked to the Chinese military, which had stolen technology blueprints, manufacturing processes, test results, business plans, pricing documents, partnership agreements and emails from more than a hundred organisations. The attackers maintained access to some networks for years. The report showed that the targets were not only defence contractors but companies in many industries.

Competitors and their agents

Most threats to the average business come not from states but from competitors, former employees and the firms or individuals they hire. Crane (2005) examined cases in which competitive intelligence gathering crossed into industrial espionage, through misrepresentation, theft of confidential documents, trespass or inducing employees to breach confidences. Some involved private investigators hired by one company to obtain a rival's information, including through searching discarded rubbish or impersonating others. Such cases damaged the reputations of the companies involved far beyond the value of the information obtained.

The line between intelligence and espionage

Businesses need to understand where legitimate competitive intelligence ends and espionage begins, both to protect themselves and to keep their own activities within bounds. Fleisher and Bensoussan (2015) and Kahaner (1996) describe the many legal and ethical sources available to competitive intelligence practitioners: published information, public filings, trade shows, customers, suppliers and industry experts. What distinguishes legitimate practice is honesty about identity and purpose, respect for confidentiality obligations, and compliance with law.

In the United States, the Economic Espionage Act of 1996 made the theft of trade secrets a federal crime, with heavier penalties where the theft benefits a foreign government. The Defend Trade Secrets Act of 2016 created a federal civil remedy, allowing companies to sue for misappropriation of trade secrets in federal courts and, in exceptional circumstances, to seek seizure of stolen material. Other countries have comparable laws. These statutes protect information only if the owner has taken reasonable measures to keep it secret. A company that leaves confidential plans unprotected may find it has no legal remedy when they are taken.

Treviño, Weaver and Reynolds (2006) review research on ethical behaviour in organisations and show that people's conduct depends heavily on the norms and incentives around them. An intelligence team under pressure to deliver may drift towards questionable methods unless clear rules are set and modelled by leaders. A business that wants to protect itself against unethical collection should also make sure its own practices are beyond reproach.

Insiders

The most damaging losses usually involve insiders. Almeling et al. (2010) analysed trade secret cases in American federal courts and found that in the large majority, the alleged misappropriator was someone the owner knew, most often an employee or business partner, rather than an unknown outsider. Cappelli, Moore and Trzeciak (2012), drawing on the CERT database of insider incidents at Carnegie Mellon University, found that theft of intellectual property by insiders often occurred within a short period before or after the person left the organisation, frequently to join a competitor or start their own business.

Band et al. (2006) compared insider cases involving information technology sabotage and espionage and identified common patterns. Insiders often had personal predispositions or grievances, experienced stressful events such as disciplinary action or disappointment over pay, and displayed concerning behaviours that colleagues noticed but did not report. Technical warning signs, such as access to information outside their normal role or unusual downloads, frequently preceded the theft. The authors concluded that many incidents could have been prevented or detected earlier if organisations had connected these signals.

Siponen and Vance (2010) found that employees who break security rules often rationalise their behaviour, believing that the information is theirs, that no harm will result or that everyone does it. Clear agreements about the ownership of work and information, reinforced by reminders at key moments such as promotions and departures, reduce the scope for such rationalisation.

How information is obtained

Figure 1 summarises common methods used to obtain business information improperly, with warning signs and defences.

How business information is targeted, and how to defend it

Most methods exploit people and routine, not advanced technology

Method	Warning signs	Defences
Insider theft	Large downloads, access outside role, departure to rival	Need-to-know, logging, exit procedures
Pretext calls and emails	Unusual requests, urgency, unknown 'colleagues'	Verify by call-back; staff training
Recruiting staff	Approaches to key staff, offers tied to information	Contracts, clear rules, open culture
Elicitation at events	Persistent questions from friendly strangers	Briefings before conferences and trade fairs
Cyber intrusion	Phishing, odd logins, data leaving the network	Multi-factor login, monitoring, patching
Partners and suppliers	Requests beyond the contract, weak controls	Due diligence, contract terms, limited access

Compiled from Nasheri (2005), Hadnagy (2018) and Cappelli et al. (2012); table by ModQu

ModQu.com

Figure 1. How business information is targeted, and how to defend it. Most methods rely on people and routine rather than advanced technology. Compiled from Nasheri (2005), Hadnagy (2018) and Cappelli et al. (2012); table by ModQu.

Social engineering and elicitation

Hadnagy (2018) describes **social engineering** as the use of influence and deception to persuade people to reveal information or take actions they otherwise would not. Common techniques include **pretexting**, in which the collector invents a plausible reason for a request, such as posing as a customer, journalist, recruiter, student or colleague from another office; and **elicitation**, in which the collector draws out information through apparently casual conversation, using flattery, deliberate errors that invite correction, or appeals to professional pride. Trade fairs, conferences and industry dinners are favoured settings because people expect to talk about their work.

Recruitment and job interviews

Competitors may approach employees with job offers and use interviews to learn about current projects. Some collectors advertise fictitious jobs to attract applicants from a target company and question them about their work. Employees should understand what they may and may not discuss with prospective employers.

Cyber intrusion

Many intrusions begin with social engineering, such as a phishing email that captures a password. Hutchins, Cloppert and Amin (2011) describe the stages through which a targeted intrusion proceeds, and how defenders can detect and disrupt it at each stage. Rid and Buchanan (2015) show that identifying who was behind an intrusion is often difficult and depends on judgement as well as technical evidence. For most businesses, the priority is detection and containment rather than attribution.

Partners, suppliers and joint ventures

Information shared with partners, suppliers, consultants and joint venture partners can leak or be misused. The National Counterintelligence and Security Center (2018) identified joint ventures and supply-chain relationships as routes through which foreign actors acquire technology. Contracts should specify confidentiality obligations, access should be limited to what the relationship requires, and partners' own security should be assessed.

Deception and counterdeception

Counterintelligence is concerned not only with theft but with deception. Opponents may try to mislead an organisation by feeding it false information. Whaley (1982) developed a general theory of deception, describing how deceivers hide the real and show the false. Godson and Wirtz (2002) examine strategic denial and deception as continuing challenges for intelligence. In business, deception can take the form of fake product rumours, misleading statements at trade events, false job advertisements designed to suggest a strategic shift, or planted information intended to provoke a costly reaction.

Heuer (1981) showed that people are especially vulnerable to deception that confirms what they already expect. Counterdeception depends on good analytic practice: evaluating sources, seeking independent corroboration, considering alternative explanations and being wary of information that is unusually convenient or arrives through a single channel.

Building a counterintelligence programme

A business counterintelligence programme need not be large. It should be led by the business, with support from security, legal, human resources and IT staff. Figure 2 sets out a simple cycle.

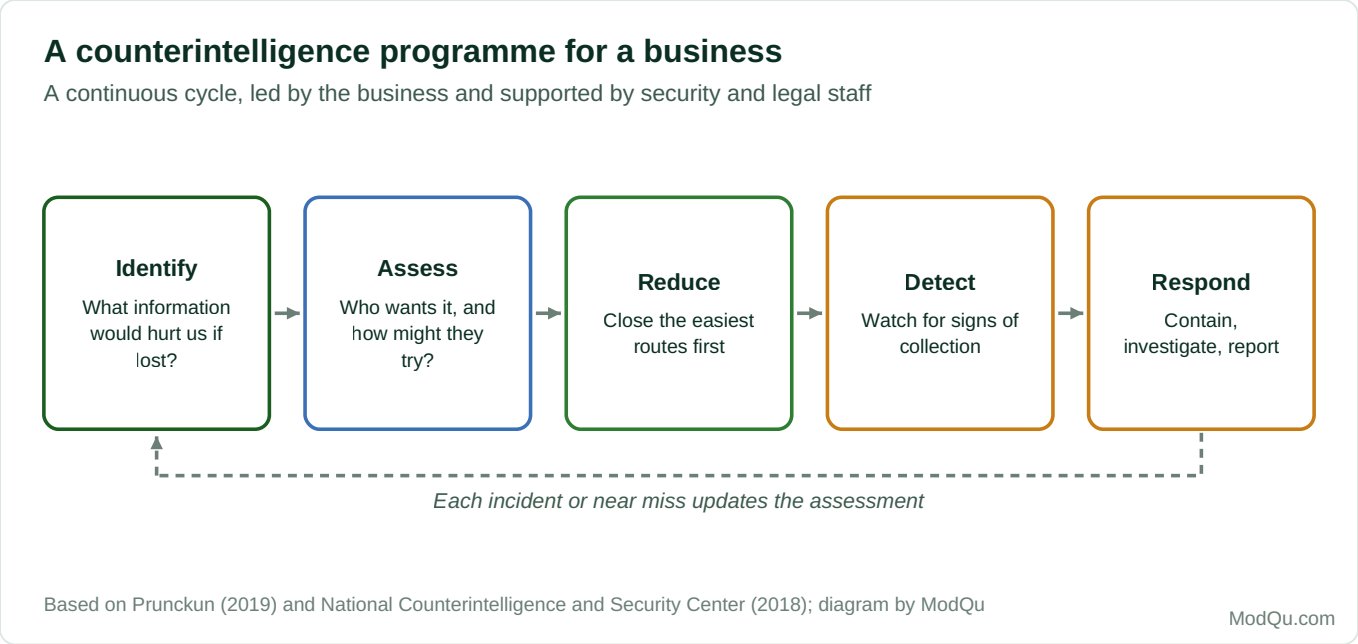


Figure 2. A counterintelligence programme for a business. Based on Prunckun (2019) and National Counterintelligence and Security Center (2018); diagram by ModQu.

Identify critical information. Not everything needs the same protection. Identify the information whose loss would cause serious harm: product designs, formulas, source code, pricing models, customer lists, acquisition plans, negotiation positions, and the intelligence team's own assessments and requirements.

Assess the threat. Consider who would want this information and how they might try to obtain it. A small engineering firm with a valuable design faces different threats from a consumer brand planning a launch.

Reduce vulnerabilities. Close the easiest routes first. Limit access to critical information to those who need it. Mark confidential material clearly, which also supports legal protection. Use non-disclosure agreements with partners and clear confidentiality clauses with employees. Brief staff who attend conferences or travel. Anderson (2020) emphasises that protection must be designed around how people actually work; Sasse, Brostoff and Weirich (2001) showed that unusable security measures are routinely bypassed.

Detect attempts. Encourage staff to report suspicious approaches, unusual questions and odd requests. Monitor access to critical information and watch for patterns such as large downloads by employees who have resigned. Review incidents and near misses.

Respond. Have a plan for what to do when a loss is suspected: who investigates, how evidence is preserved, when lawyers are involved and when law enforcement is notified. Quick action can limit damage and preserve legal remedies.

Culture and reporting

The most effective counterintelligence measure is a workforce that recognises approaches and reports them. This depends on culture. Edmondson (1999) showed that teams with high **psychological safety**, where people feel safe to speak up without fear of blame, are more likely to report problems and learn from them. Employees who fear they will be blamed for having been approached, or for having said too much at a conference, will stay silent. Organisations should thank staff for reporting, treat honest mistakes as learning opportunities, and share anonymised examples so that others learn to recognise similar approaches.

Departures and arrivals

Moments of transition carry particular risk. When an employee resigns, especially to join a competitor, organisations should promptly review and adjust their access, remind them of their confidentiality obligations, recover company devices and documents, and review recent access to critical information. Exit interviews provide an opportunity to reinforce obligations and to ask about any approaches the person received.

Arrivals carry a mirror-image risk. A new employee from a competitor may bring confidential information, intentionally or not. Using it can expose the hiring company to legal action and reputational harm. New employees should be told clearly not to bring or use a former employer's confidential information, and managers should not ask them to.

Proportionality

Counterintelligence measures have costs. Excessive secrecy slows work, hinders collaboration and can create a culture of suspicion that damages morale and innovation. Monitoring employees raises legal and ethical questions about privacy. Measures should be proportionate to the value of the information and the likelihood of threats. Most businesses need sensible protection of a small amount of critical information, awareness among staff, and clear procedures, not elaborate security operations.

Travel, conferences and visitors

Trade fairs, conferences and business travel are among the most common settings for information gathering. People are relaxed, proud of their work and keen to network, and conversations move quickly from general topics to specific ones. The National Counterintelligence and Security Center (2018) advises staff travelling abroad to carry only the information and devices they need, to assume that hotel rooms, public Wi-Fi and borrowed charging cables may be insecure, and to report unusual contacts on their return.

Visitors to company premises raise similar issues. A plant tour for a prospective customer, a delegation from a partner or a group of students can all include people whose interest goes beyond the stated purpose. Simple measures help: agree in advance what will be shown, escort visitors, ask them not to take photographs in sensitive areas, and brief the hosts on what not to discuss. None of this needs to be hostile; most visitors are exactly who they say they are.

Protecting the intelligence team's own work

An intelligence team holds some of the most sensitive information in the business: what leaders want to know, what they fear and which options they are considering. A competitor who learned the team's requirements would learn the company's strategy. Herman (1996) notes that protecting one's own intelligence effort is part of intelligence itself, not an add-on. In practice this means restricting circulation of requirements and assessments, being careful about what questions are asked of outside sources, and making sure that contractors who gather information on the company's behalf do not reveal who the client is or why it is interested. Fleisher and Bensoussan (2015) make the same point about competitive analysis: the questions an analyst asks can reveal as much as the answers they receive.

Working with legal, HR and IT

Counterintelligence crosses departmental lines, and gaps between departments are where losses happen. Lawyers advise on what counts as a trade secret and on the reasonable measures needed to preserve legal protection; Almeling and colleagues found that many trade secret cases turn on whether the owner took such measures (Almeling et al., 2010). Human resources staff manage hiring, confidentiality agreements, exits and investigations of staff conduct. IT staff control access and keep the logs that reveal unusual activity. Cappelli et al. (2012) recommend that these groups meet regularly, share warning signs and agree in advance who does what when an incident occurs.

Questions to ask about critical information

A short review of each item of critical information can be organised around a few questions:

1. What harm would follow if a competitor obtained it, and how soon?
2. Who has access to it now, and do they all need it?
3. Where is it stored, copied and sent, including to partners and suppliers?
4. Is it marked and covered by agreements that would support legal action?
5. Would we know if it had been copied or taken, and who would notice first?

Answers that are uncertain point to the next improvement.

A business illustration

A medium-sized manufacturer of specialist medical devices is preparing to launch a new product. During a trade fair, an engineer is approached by a friendly visitor claiming to be a university researcher, who asks detailed questions about testing methods. A week later, the engineer receives an email from the same person offering a paid consultancy. The engineer, who had attended a short counterintelligence briefing before the fair, reports both contacts. The company's security lead finds that the "researcher" has no university affiliation, and that a competitor has recently advertised for engineers with exactly the engineer's expertise.

At the same time, a routine review of access logs shows that a product manager who has just resigned downloaded the full launch plan and pricing model the day before resigning. The company's lawyers contact the manager, who returns the files and confirms in writing that no copies were kept. The company tightens access to launch documents, briefs all staff attending future events, and adds a step to its resignation procedure to review recent access. The launch proceeds without any sign of leaked information.

Common mistakes

- **Assuming the company is too small to be a target.** Smaller firms with valuable technology are often targeted because their defences are weaker.
- **Protecting everything equally.** Spreading effort thinly leaves critical information under-protected.
- **Ignoring insiders.** Most losses involve people the company knows.
- **Punishing reporting.** Staff who are blamed for being approached will not report the next approach.
- **Neglecting legal protection.** Without reasonable secrecy measures, trade secret laws may offer no remedy.
- **Using questionable methods in return.** Responding to espionage with unethical tactics exposes the company to legal and reputational harm.

Conclusion

Business counterintelligence protects what an organisation knows and plans from those who would take it improperly. The main threats come not from exotic technology but from people: insiders who leave with information, collectors who use deception and conversation, and attackers who exploit routine weaknesses. A proportionate programme identifies the information that matters most, understands who might want it, closes the easiest routes, encourages staff to report approaches, and responds quickly when something goes wrong. Combined with high ethical standards in the company's own intelligence work, it allows a business to compete on knowledge without losing it.

References

Almeling, D. S., Snyder, D. W., Sapoznikow, M., McCollum, W. E., & Weader, J. (2010). A statistical analysis of trade secret litigation in federal courts. *Gonzaga Law Review, 45*(2), 291–334.

Anderson, R. (2020). *Security engineering: A guide to building dependable distributed systems* (3rd ed.). Wiley.

Band, S. R., Cappelli, D. M., Fischer, L. F., Moore, A. P., Shaw, E. D., & Trzeciak, R. F. (2006). *Comparing insider IT sabotage and espionage: A model-based analysis* (CMU/SEI-2006-TR-026). Software Engineering Institute, Carnegie Mellon University.

Cappelli, D. M., Moore, A. P., & Trzeciak, R. F. (2012). *The CERT guide to insider threats: How to prevent, detect, and respond to information technology crimes*. Addison-Wesley.

Crane, A. (2005). In the company of spies: When competitive intelligence gathering becomes industrial espionage. *Business Horizons, 48*(3), 233–240. https://doi.org/10.1016/j.bushor.2004.11.005

Defend Trade Secrets Act of 2016, Pub. L. No. 114-153, 130 Stat. 376 (2016).

Economic Espionage Act of 1996, 18 U.S.C. §§ 1831–1839 (1996).

Edmondson, A. (1999). Psychological safety and learning behavior in work teams. *Administrative Science Quarterly, 44*(2), 350–383. https://doi.org/10.2307/2666999

Fleisher, C. S., & Bensoussan, B. E. (2015). *Business and competitive analysis: Effective application of new and classic methods* (2nd ed.). Pearson Education.

Godson, R., & Wirtz, J. J. (Eds.). (2002). *Strategic denial and deception: The twenty-first century challenge*. Transaction.

Hadnagy, C. (2018). *Social engineering: The science of human hacking* (2nd ed.). Wiley.

Herman, M. (1996). *Intelligence power in peace and war*. Cambridge University Press.

Heuer, R. J., Jr. (1981). Strategic deception and counterdeception: A cognitive process approach. *International Studies Quarterly, 25*(2), 294–327.

Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *Leading Issues in Information Warfare & Security Research, 1*(1), 80–106.

Kahaner, L. (1996). *Competitive intelligence: How to gather, analyze, and use information to move your business to the top*. Simon & Schuster.

Mandiant. (2013). *APT1: Exposing one of China's cyber espionage units*. Mandiant.

Nasheri, H. (2005). *Economic espionage and industrial spying*. Cambridge University Press.

National Counterintelligence and Security Center. (2018). *Foreign economic espionage in cyberspace*.

Prunckun, H. (2019). *Counterintelligence theory and practice* (2nd ed.). Rowman & Littlefield.

Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. *Journal of Strategic Studies, 38*(1–2), 4–37. https://doi.org/10.1080/01402390.2014.977382

Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the "weakest link": A human/computer interaction approach to usable and effective security. *BT Technology Journal, 19*(3), 122–131. https://doi.org/10.1023/A:1011902718709

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly, 34*(3), 487–502. https://doi.org/10.2307/25750688

Treviño, L. K., Weaver, G. R., & Reynolds, S. J. (2006). Behavioral ethics in organizations: A review. *Journal of Management, 32*(6), 951–990. https://doi.org/10.1177/0149206306294258

Whaley, B. (1982). Toward a general theory of deception. *Journal of Strategic Studies*, *5*(1), 178–192. https://doi.org/10.1080/01402398208437106