INTELLIGENCE · ORGANISATIONAL INTELLIGENCE

Interagency Intelligence Sharing Protocols and Knowledge Interoperability

Many intelligence failures happen not because information was missing but because it was held by one organisation and needed by another. This article explains why sharing between agencies and organisations is difficult, what inquiries into past failures have found, and how protocols and interoperability standards make shared knowledge usable, with lessons for businesses that share intelligence with partners and across divisions.

ModQu research article · 2,818 words · 24 references (APA 7th edition)

When an intelligence failure is investigated, a familiar pattern often emerges. The information needed to prevent the failure existed, but it was spread across different organisations, none of which had the whole picture. One agency knew one fact, another knew a second, and nobody put them together. Sometimes the information was not shared because of rules; sometimes because of habit, mistrust or incompatible systems; sometimes because nobody realised that another organisation needed it.

This article examines **interagency intelligence sharing**: the movement of intelligence knowledge between separate organisations, or between separate parts of one large organisation. It looks at what inquiries have found, why sharing is difficult, what **protocols** govern it and what **knowledge interoperability** requires: the ability of one organisation's knowledge to be understood and used by another. The examples come mainly from government, where the problem has been studied most closely, but the lessons apply to businesses that share intelligence across divisions, with partners in a supply chain or within industry groups.

What inquiries have found

The inquiry into the attacks of 11 September 2001 found that American agencies held pieces of relevant information but did not share or combine them. The National Commission on Terrorist Attacks Upon the United States (2004) described a failure to "connect the dots" and recommended a shift from a culture of "need to know" towards one of "need to share". Zegart (2007) argued that the deeper causes lay in organisational structures, incentives and cultures that had developed over decades and that resisted change even after earlier warnings. The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (2005) found related problems in the assessment of Iraq's weapons programmes, including poor sharing of doubts about key sources between agencies.

The response included the Intelligence Reform and Terrorism Prevention Act of 2004, which created the Director of National Intelligence with responsibility for integrating the intelligence community and an information sharing environment. The Markle Foundation Task Force on National Security in the Information Age (2003) had argued for a decentralised, trusted network in which agencies could find and share information horizontally, with built-in protections for privacy and civil liberties.

The problem is not limited to national security. In the United Kingdom, the inquiry into the death of Victoria Climbié found that the child had been in contact with many agencies, including social services, the police and hospitals, yet none had acted on the information they held, partly because information was not shared or brought together (Laming, 2003). The Bichard inquiry, following the Soham murders, found that police forces had held information about the offender's previous contacts with the police but that it had not been shared or recorded in a way that would have prevented the offender's employment at a school (Bichard, 2004). Munro (2011), reviewing child protection, warned that responding to such failures simply by adding procedures and forms can make matters worse, by turning professionals' attention to compliance rather than to understanding the situation.

Why sharing is difficult

Research on information sharing between public organisations identifies several kinds of barrier. Yang and Maxwell (2011), reviewing the literature, group them into interpersonal, organisational and technical factors. Dawes (1996) found that managers saw clear benefits in sharing, such as better decisions and reduced duplication, but also real risks, such as loss of control, misuse of data and damage to their organisation's reputation. Bardach (1998), studying collaboration between public agencies, found that it depends less on formal agreements than on the "craftsmanship" of managers who build trust, find shared purposes and work around obstacles.

Barriers to intelligence sharing

Most barriers are organisational and cultural, not technical

Barrier	Examples	Typical remedies
Technical	Different systems, formats, security levels	Common formats, secure links
Organisational	Own priorities; benefits go to others	Shared goals, credit for sharing
Legal	Privacy and secrecy rules, unclear authority	Clear legal basis, guidance
Cultural	Need to know, mistrust, protecting sources	Joint work, secondments, feedback

Compiled from Dawes (1996), Bardach (1998) and Yang and Maxwell (2011); table by ModQu

ModQu.com

Figure 1. Barriers to intelligence sharing and their remedies. Most barriers are organisational and cultural rather than technical. Compiled from Dawes (1996), Bardach (1998) and Yang and Maxwell (2011); table by ModQu.

Technical barriers. Organisations use different systems, data formats, vocabularies and security levels. Even when they want to share, their data may not fit together.

Organisational barriers. Each organisation has its own priorities, budgets and performance measures. Sharing takes time and effort, and the benefits often go to the recipient rather than the provider. Zegart (2007) emphasises that agencies are rewarded for their own successes, not for helping others.

Legal barriers. Laws on privacy, secrecy and the use of data restrict what may be shared and with whom. Some restrictions are essential; others are misunderstood or applied too cautiously. Bichard (2004) found that confusion about data protection law had contributed to the failure to retain and share information.

Cultural barriers. Intelligence organisations have traditionally protected their sources and methods through the **need-to-know** principle, which limits access to those with a specific requirement. This protects sources but makes it hard to share with people whose need is not obvious in advance. Lowenthal (2022) notes the persistent tension between protecting sources and ensuring that information reaches those who need it. Trust between organisations also matters: agencies share more with partners they know and trust.

Knowledge is sticky

Even within a single organisation, knowledge does not flow easily. Szulanski (1996) studied the transfer of best practices within firms and found that the main barriers were not motivational but related to knowledge itself: recipients lacked the background to absorb it, the causes of success were unclear, and relationships between source and recipient were difficult. Szulanski called this **stickiness**. Davenport and Prusak (1998) similarly emphasise that knowledge is tied to context and to people, and that moving it requires shared language and trust.

Intelligence knowledge is especially sticky. An assessment depends on sources, assumptions and context that the recipient may not see. A fact reported by one agency may be interpreted differently by another. Sharing raw data without context can mislead; sharing finished assessments without the underlying evidence can make it hard for the recipient to judge them.

Knowledge interoperability

Interoperability is the ability of different systems and organisations to exchange information and use it. It has several layers, each of which must work for sharing to be effective.

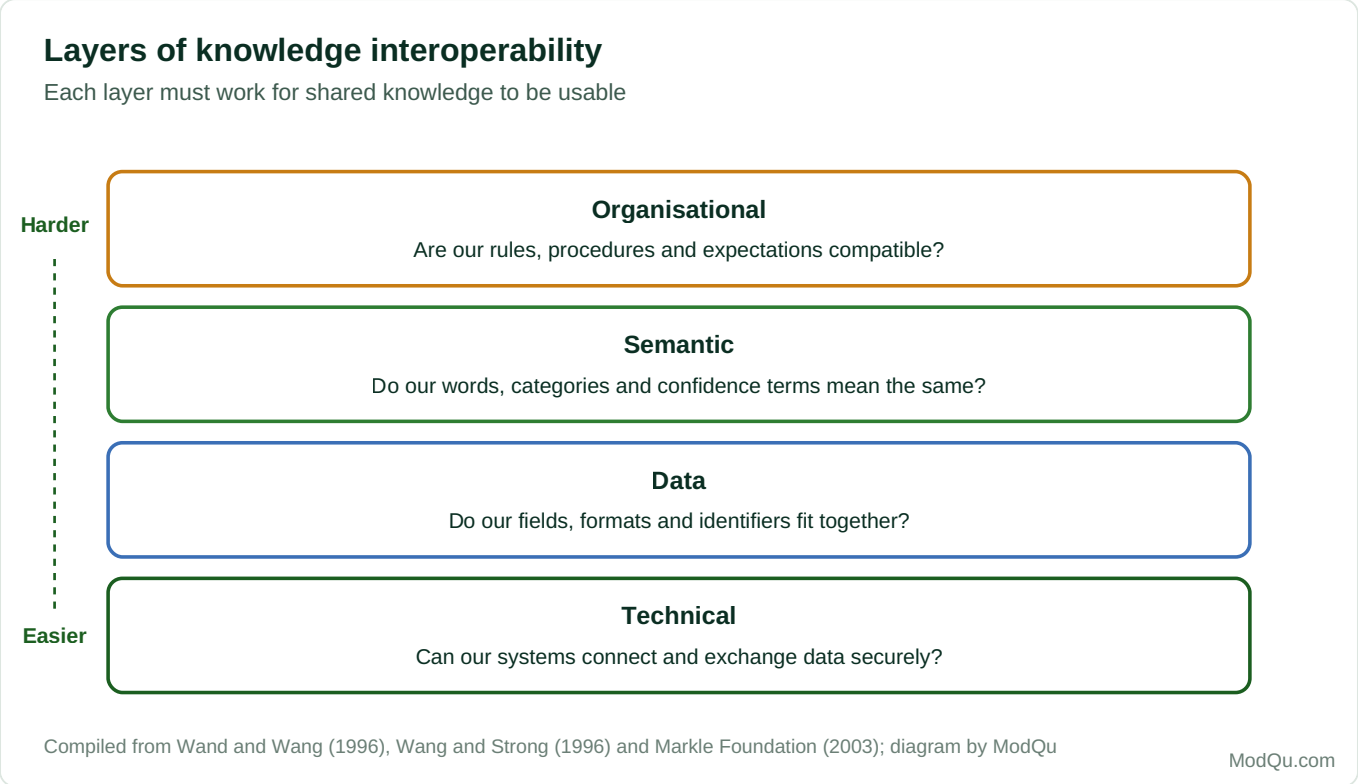


Figure 2. Layers of knowledge interoperability. Technical connection is the easiest layer; shared meaning and shared rules are harder and matter more. Compiled from Wand and Wang (1996), Wang and Strong (1996) and Markle Foundation Task Force on National Security in the Information Age (2003); diagram by ModQu.

Technical interoperability means that systems can connect and exchange data securely. This includes networks, security accreditation and file formats.

Data interoperability means that data is structured in compatible ways, with agreed fields and formats for names, dates, places and identifiers. Without this, combining records from different sources produces errors and duplicates.

Semantic interoperability means that the meaning of information is shared. Two organisations may use the same word, such as "threat level" or "confirmed", with different meanings. Agreed vocabularies, definitions and standard expressions of probability and confidence help. Wand and Wang (1996) show that data quality depends on how well data represents the real world it describes, and that mismatches in meaning are a major source of error.

Organisational interoperability means that the rules, procedures and expectations of the organisations are compatible: who may share what with whom, how requests are handled, how quickly, and with what protections.

Data quality is a further requirement. Wang and Strong (1996) found that data users judge quality not only on accuracy but on relevance, timeliness, completeness, interpretability and accessibility. Shared intelligence that is accurate but out of date, incomplete or hard to interpret may be of little use.

Protocols for sharing

A **sharing protocol** is an agreed set of rules for how intelligence will be exchanged. Good protocols typically cover:

- **Purpose.** Why information is shared and what it may be used for.
- **Scope.** Which kinds of information are covered.
- **Handling markings.** How sensitivity and restrictions are labelled, and what each label means for storage, onward sharing and use.
- **Source protection.** How the identity and safety of sources are protected, for example by sharing assessments rather than raw reports, or by removing identifying details.
- **Requests and responses.** How one organisation asks another for information and how quickly it can expect a reply.
- **Context.** What background, confidence levels and caveats must accompany shared items.
- **Feedback.** How recipients report back on the usefulness and accuracy of shared information.
- **Legal basis and accountability.** The legal authority for sharing, the records to be kept and the oversight that applies.

Omand (2010) notes that international intelligence partnerships rely on a principle often called the **third-party rule**: information received from one partner is not passed on to another without permission. This protects the originator and sustains trust. Similar rules apply in many business arrangements, such as industry information-sharing groups.

Born and Leigh (2005) emphasise that sharing between agencies, particularly across borders, must be subject to oversight, since information shared with partners may be used in ways that would not be permitted at home. Data protection law also applies to sharing personal data: in Europe, the General Data Protection Regulation requires a lawful basis for each transfer and imposes conditions on transfers outside the European Union (European Union, 2016).

What to share: raw data or assessments?

A recurring choice is whether to share raw information, finished assessments or something in between. Each has advantages and risks.

Raw data lets the recipient analyse it for their own purposes and combine it with their own holdings. But raw data may expose sources, may be misread without context and may be too voluminous to use. It also raises the greatest privacy concerns when it contains personal information.

Finished assessments are easier to use, protect sources better and carry the provider's expertise. But the recipient cannot check the reasoning or reuse the evidence for a different question, and may give the assessment more or less weight than it deserves.

A middle path is to share assessments together with a summary of the evidence, its sources described in general terms, the confidence level and the key assumptions. Recipients who need more can request it under the protocol. Fingar (2011) notes that making the basis of judgements visible, including the quality of sources, improved the usefulness and credibility of shared products in the American intelligence community.

Questions to ask before a sharing agreement

Before agreeing to share intelligence with another organisation or division, it helps to ask:

1. What decisions will the shared information support, on each side?
2. What exactly will be shared, and what will not?
3. What legal basis allows the sharing, and what records must be kept?
4. How will sources and personal data be protected?
5. How will each side describe confidence, and do the terms mean the same?
6. What happens if one side breaches the agreement?
7. How will both sides know, after six months, whether the sharing is working?

Measuring whether sharing works

Sharing arrangements are easy to set up and hard to evaluate. Counting the number of items shared measures activity, not value. More useful measures include how often shared information was used in decisions or products, how quickly requests were answered, how often recipients found shared items unclear or out of date, and whether recipients report learning things they would not otherwise have known. Recording instances where shared information made a difference, and instances where information that should have been shared was not, gives a practical picture of performance. Regular review of these measures, ideally jointly by both partners, keeps the arrangement focused on its purpose.

Sharing in business

Businesses face the same problems in different forms.

Across divisions. In large companies, the sales team may know that a competitor is discounting heavily in one region, while the strategy team is unaware. Different divisions may maintain separate competitor files with conflicting information.

Along the supply chain. Lee et al. (2000) showed that sharing demand information between a retailer and its supplier can create substantial value, by reducing inventory and costs, especially when demand is variable and correlated over time. Yet companies are often reluctant to share for fear of losing bargaining power.

Within industries. In cybersecurity, companies share information about threats through industry groups and platforms. Wagner et al. (2019), in a survey of cyber threat intelligence sharing, found that the main obstacles were trust, legal uncertainty, the quality and timeliness of shared data, and the lack of common standards, and that structured formats and clear rules on use and attribution help.

The same remedies apply as in government: clear protocols, common vocabularies, attention to data quality, legal clarity and above all trust.

Central hubs and networks

Organisations have tried two broad models for sharing. In a **hub** model, a central body collects information from many providers, combines it and distributes products. Fusion centres, which bring together staff from several agencies in one place, are an example. Hubs make it easier to see the whole picture and to apply common standards, but they can become bottlenecks and may lose touch with the expertise of the providers. In a **network** model, organisations share directly with one another according to common rules, often through shared platforms. The Markle Foundation Task Force on National Security in the Information Age (2003) favoured this approach, arguing that it is more resilient and adapts better to new threats. In practice, many arrangements combine the two: a small central team sets standards and maintains shared tools, while most sharing happens directly between those who hold and need the information.

Building trust

Trust is the foundation of sharing. Bardach (1998) found that successful collaboration grows through repeated interaction in which partners show that they will use shared information responsibly and reciprocate. Treverton (2003) argues that intelligence organisations need to move from hierarchies that hoard information towards networks that share it, which requires both new technology and new habits. Fingar (2011), who led analytic integration across the American intelligence community, describes how joint work on common products, shared standards and rotation of staff between agencies helped build trust and understanding. Gill and Phythian (2018) note that sharing also creates new risks, including the spread of errors and the use of shared intelligence for purposes the provider would not support, which is why trust must be backed by rules.

Practical steps to build trust include:

- **Start small.** Begin with low-risk information and expand as confidence grows.
- **Reciprocate.** Give as well as receive.
- **Give feedback.** Tell providers how their information was used and whether it was useful.

- **Exchange people.** Secondments and joint teams build personal relationships and understanding of partners' work.
- **Honour restrictions.** A single breach of a handling restriction can end a sharing relationship.

Common mistakes

- **Treating sharing as a technical problem.** New systems alone rarely solve sharing failures, which are usually organisational and cultural.
- **Sharing without context.** Raw data without sources, confidence or caveats can mislead.
- **Adding procedures without understanding.** As Munro (2011) warned, more forms can increase compliance work without improving judgement.
- **Over-restricting.** Excessive caution about law or security can prevent sharing that is lawful and necessary.
- **Under-protecting.** Careless sharing can expose sources, breach privacy and destroy trust.
- **No feedback loop.** Providers who never learn whether their information helped stop providing it.

A business illustration

A multinational food company has separate intelligence functions in its three regional divisions and a small central strategy team. Each division tracks competitors and markets, but uses its own templates, terms and systems. When a global competitor launches a campaign in several regions at once, each division reports it separately, with conflicting estimates of its scale, and the central team takes a week to reconcile them.

The company sets up a sharing protocol. It agrees common competitor and market profiles with standard fields, a shared vocabulary for confidence levels and a single platform where all divisions post significant developments. Each item must include its source, date and confidence level. Divisions agree to respond to requests from each other within two working days. Handling markings identify information that must not leave a division, such as details of commercial negotiations. A monthly call between the regional intelligence leads reviews shared items and discusses disagreements.

Within a year, the central team can produce a global view of competitor activity in days rather than weeks. Divisions report that they learn early about competitor moves in other regions, which often foreshadow moves in their own. The most important change, the leads agree, is not the platform but the regular contact, which has built the trust needed for people to share uncertain and early information.

Conclusion

Intelligence failures often arise not from a lack of information but from a failure to bring together what different organisations know. Sharing is difficult for technical, organisational, legal and cultural reasons, and knowledge is sticky even when people want to share it. Effective sharing requires interoperability at several levels, from technical connections to shared meanings and compatible rules, together with clear protocols covering purpose, handling, source protection, context and accountability. Above all, it requires trust, built through repeated, reciprocal and well-governed exchange. Businesses that share intelligence across divisions, with partners or within industries face the same challenges and can apply the same lessons.

References

Bardach, E. (1998). *Getting agencies to work together: The practice and theory of managerial craftsmanship*. Brookings Institution Press.

Bichard, M. (2004). *The Bichard inquiry report* (HC 653). The Stationery Office.

Born, H., & Leigh, I. (2005). *Making intelligence accountable: Legal standards and best practice for oversight of intelligence agencies*. Publishing House of the Parliament of Norway.

Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction. (2005). *Report to the President of the United States*. U.S. Government Printing Office.

Davenport, T. H., & Prusak, L. (1998). *Working knowledge: How organizations manage what they know*. Harvard Business School Press.

Dawes, S. S. (1996). Interagency information sharing: Expected benefits, manageable risks. *Journal of Policy Analysis and Management, 15*(3), 377–394. https://doi.org/10.1002/(SICI)1520-6688(199622)15:3<377::AID-PAM3>3.0.CO;2-F

European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). *Official Journal of the European Union, L 119*, 1–88.

Fingar, T. (2011). *Reducing uncertainty: Intelligence analysis and national security*. Stanford University Press.

Gill, P., & Phythian, M. (2018). *Intelligence in an insecure world* (3rd ed.). Polity Press.

Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638 (2004).

Laming, H. (2003). *The Victoria Climbié inquiry: Report of an inquiry by Lord Laming* (Cm 5730). The Stationery Office.

Lee, H. L., So, K. C., & Tang, C. S. (2000). The value of information sharing in a two-level supply chain. *Management Science, 46*(5), 626–643. https://doi.org/10.1287/mnsc.46.5.626.12047

Lowenthal, M. M. (2022). *Intelligence: From secrets to policy* (9th ed.). CQ Press.

Markle Foundation Task Force on National Security in the Information Age. (2003). *Creating a trusted information network for homeland security*. Markle Foundation.

Munro, E. (2011). *The Munro review of child protection: Final report. A child-centred system* (Cm 8062). The Stationery Office.

National Commission on Terrorist Attacks Upon the United States. (2004). *The 9/11 Commission report*. W. W. Norton.

Omand, D. (2010). *Securing the state*. Hurst.

Szulanski, G. (1996). Exploring internal stickiness: Impediments to the transfer of best practice within the firm. *Strategic Management Journal, 17*(S2), 27–43. https://doi.org/10.1002/smj.4250171105

Treverton, G. F. (2003). *Reshaping national intelligence for an age of information*. Cambridge University Press.

Wagner, T. D., Mahbub, K., Palomar, E., & Abdallah, A. E. (2019). Cyber threat intelligence sharing: Survey and research directions. *Computers & Security, 87*, Article 101589. https://doi.org/10.1016/j.cose.2019.101589

Wand, Y., & Wang, R. Y. (1996). Anchoring data quality dimensions in ontological foundations. *Communications of the ACM, 39*(11), 86–95. https://doi.org/10.1145/240455.240479

Wang, R. Y., & Strong, D. M. (1996). Beyond accuracy: What data quality means to data consumers. *Journal of Management Information Systems, 12*(4), 5–33. https://doi.org/10.1080/07421222.1996.11518099

Yang, T.-M., & Maxwell, T. A. (2011). Information-sharing in public organizations: A literature review of interpersonal, intra-organizational and inter-organizational success factors. *Government Information Quarterly, 28*(2), 164–175. https://doi.org/10.1016/j.giq.2010.06.008

Zegart, A. B. (2007). *Spying blind: The CIA, the FBI, and the origins of 9/11*. Princeton University Press.