INTELLIGENCE · ORGANISATIONAL INTELLIGENCE

Information Security and the Protection of Intelligence Assets

Intelligence is valuable precisely because others do not have it, which makes it a target. This article explains how organisations protect their intelligence assets: the core principles of information security, the main threats, the human factors behind most breaches, the frameworks that structure a security programme, and practical steps for intelligence teams of any size.

ModQu research article · 2,907 words · 25 references (APA 7th edition)

An intelligence function gathers and produces some of the most sensitive information an organisation holds: assessments of competitors, plans for new markets, details of negotiations, customer research, the identities of sources and contacts. Its value lies partly in exclusivity. A competitor who obtains a company's market assessment, pricing analysis or acquisition shortlist gains the advantage the company paid to create. A regulator, journalist or criminal who obtains confidential data can cause legal, reputational and financial harm. Protecting **intelligence assets** is therefore part of the intelligence function's job, not an afterthought left to the IT department.

This article explains the principles of information security as they apply to intelligence work, the threats intelligence assets face, the human factors behind most failures, the frameworks that structure a security programme, and the practical steps any intelligence team can take.

What needs protecting

Intelligence assets take several forms:

- **Raw information**: collected documents, data sets, interview notes, survey results, purchased reports.
- **Finished products**: assessments, briefs, forecasts, profiles of competitors and customers.
- **Sources and methods**: who provided information, how it was obtained, which tools and techniques the team uses.
- **Requirements**: the questions the organisation is asking, which reveal its plans and concerns.
- **Personal data**: information about customers, respondents, employees and contacts, which carries legal obligations.
- **Systems and accounts**: the tools, databases and credentials through which all of the above is accessed.

The last two points are often underestimated. Requirements reveal strategy: a competitor who learns that a company is researching a particular region or product can infer its plans. Accounts and systems are the routes through which most attacks proceed.

Core principles

Information security is traditionally described by three properties. Anderson (2020), in a standard text on security engineering, explains them and the trade-offs between them. Figure 1 applies them to intelligence work.

Protecting intelligence assets: three properties

Confidentiality, integrity and availability applied to intelligence work

Property	What it protects	Typical threat	Example controls
Confidentiality	Sources, plans, client data, assessments	Theft, leaks, careless sharing	Access limits, encryption, need-to-know
Integrity	Accuracy of data and analysis	Tampering, planted information	Change logs, source checks, backups
Availability	Access when decisions are made	Ransomware, outages, lost keys	Backups, redundancy, recovery plans

Based on Anderson (2020); examples by ModQu

ModQu.com

Figure 1. Protecting intelligence assets: three properties. Intelligence teams tend to focus on confidentiality, but integrity and availability matter as much. Based on Anderson (2020); examples by ModQu.

Confidentiality means that information is accessible only to those authorised to see it. **Integrity** means that information is accurate and has not been altered without authorisation. **Availability** means that information and systems are accessible when needed. Intelligence teams naturally focus on confidentiality, but integrity is equally important: an assessment based on tampered or planted information is worse than no assessment at all. Availability matters when a decision is due and the files are locked by ransomware.

Saltzer and Schroeder (1975) set out design principles for protecting information in computer systems that remain influential today. Among them are **least privilege**, giving each user and program only the access it needs; **fail-safe defaults**, denying access unless it is explicitly granted; **complete mediation**, checking every access rather than trusting earlier checks; **separation of privilege**, requiring more than one condition or person for sensitive actions; and **psychological acceptability**, designing protection so that people use it routinely and correctly. The last principle is often forgotten and explains many failures.

Schneier (2000) argued that security is a process, not a product. No single technology makes an organisation secure. Security depends on people, procedures and technology working together, and on continuous attention as threats change.

The threat landscape

Who attacks, and why

Threats to intelligence assets come from several directions:

- **Competitors and their agents**, seeking plans, pricing, research and customer information.
- **Criminals**, seeking data to sell, accounts to exploit or systems to hold for ransom.
- **State-sponsored groups**, seeking intellectual property and strategic information.
- **Insiders**, current or former employees and contractors who misuse their access.
- **Accidents**, such as misdirected emails, lost devices and misconfigured systems.

Mandiant (2013), a security company, published a detailed report on a group it linked to the Chinese military, which had stolen large volumes of intellectual property and business information from more than a hundred organisations across many industries over several years. The report showed that the attackers maintained access to some victims for long periods and took plans, negotiation positions and technical data. It illustrated that commercial information, not only government secrets, is a target of sophisticated espionage.

Attackers also exploit weakly protected devices at scale. Kolias et al. (2017) analysed the Mirai botnet, which took over large numbers of internet-connected cameras and other devices using default passwords and used them to launch massive attacks that disrupted major websites. The lesson for intelligence teams is that any connected device, however minor, can become a route into a network.

Attributing attacks is difficult. Rid and Buchanan (2015) describe attribution as a process of judgement drawing on technical evidence, operational patterns and strategic context, rarely reaching certainty. For most organisations, the practical priority is not identifying the attacker but closing the weaknesses that allowed the attack.

How attacks proceed

Hutchins, Cloppert and Amin (2011) described the **intrusion kill chain**, a model of the stages through which a targeted attack proceeds: reconnaissance, preparing a weapon, delivering it, exploiting a weakness, installing access, establishing remote control, and acting on objectives. Defenders who understand the chain can look for signs at each stage and interrupt the attack before it succeeds. The MITRE ATT&CK knowledge base catalogues the specific tactics and techniques attackers use at each stage, based on observed attacks (Strom et al., 2018). The diamond model of intrusion analysis describes each attack event in terms of the adversary, their capability, the infrastructure they use and the victim, helping analysts link related events (Caltagirone et al., 2013).

These models are themselves forms of intelligence. **Cyber threat intelligence**, the collection and analysis of information about attackers, their methods and their targets, helps organisations anticipate and defend against attacks. Tounsi and Rais (2018) survey its forms, from technical indicators such as malicious addresses to strategic assessments of which groups are likely to target a given sector.

The cost of breaches

Breaches are costly. IBM's (2024) annual study of data breaches estimated the global average cost of a breach at several million US dollars, including detection, response, lost business and regulatory consequences. The Verizon (2024) data breach investigations report, which analyses thousands of incidents each year, found that a large majority of breaches involved a human element, such as errors, misuse of privileges, stolen credentials or social engineering.

The human factor

Social engineering

Many attacks do not break technical defences but persuade people to bypass them. **Social engineering** uses deception to manipulate people into revealing information, granting access or taking harmful actions. Hadnagy (2018) describes the main techniques: phishing emails that impersonate trusted senders, telephone calls from apparent IT staff or executives, pretexts that create urgency or authority, and physical approaches such as following employees through secure doors. Intelligence staff are attractive targets because they hold sensitive information and often communicate with outsiders as part of their work.

Usable security

Security measures that are difficult to use are often bypassed. Sasse, Brostoff and Weirich (2001) studied password practices and found that users were not careless by nature; rather, organisations imposed rules, such as frequent changes and complex passwords for many systems, that exceeded human memory. Users responded by writing passwords down or reusing them. The authors argued that users should be treated as partners in security, not as the "weakest link".

Herley (2009) went further, arguing that users often rationally reject security advice because the time and effort it demands exceed the expected benefit to them. Security teams that ignore these costs produce rules that are routinely broken. Effective security makes the secure way the easy way.

Compliance and its limits

Why do employees follow or break security policies? Bulgurcu, Cavusoglu and Benbasat (2010) found that employees' intentions to comply were shaped by their beliefs about the benefits of compliance, the costs of compliance and the costs of non-compliance, and by their general awareness of security. Training that improves awareness and explains why rules matter increases compliance. Siponen and Vance (2010) found that employees who break security policies often justify it to themselves through **neutralisation**, telling themselves that the rule is unreasonable, that no harm will result, or that the work demanded it. Effective programmes address these justifications directly.

Insiders

Insiders are among the most damaging threats because they already have access. Cappelli, Moore and Trzeciak (2012), drawing on hundreds of cases collected by the CERT programme at Carnegie Mellon University, describe insider threats including theft of intellectual property, sabotage and fraud. Band et al. (2006) compared cases of insider sabotage and

espionage and found common patterns: personal predispositions, stressful events, concerning behaviours that were observed but not acted on, and technical warning signs such as unusual access. Many insider thefts of intellectual property occur around the time an employee leaves for a competitor. Almeling et al. (2010), analysing trade secret litigation in American federal courts, found that in most cases the alleged misappropriator was someone the owner knew, usually an employee or business partner.

Frameworks for a security programme

Organisations do not need to design security from scratch. Several frameworks provide structure.

The National Institute of Standards and Technology (2024) Cybersecurity Framework 2.0 organises security activities into six functions, shown in Figure 2. The 2024 revision added **Govern** to the original five functions, emphasising that security strategy, roles and policy must be set by leadership.

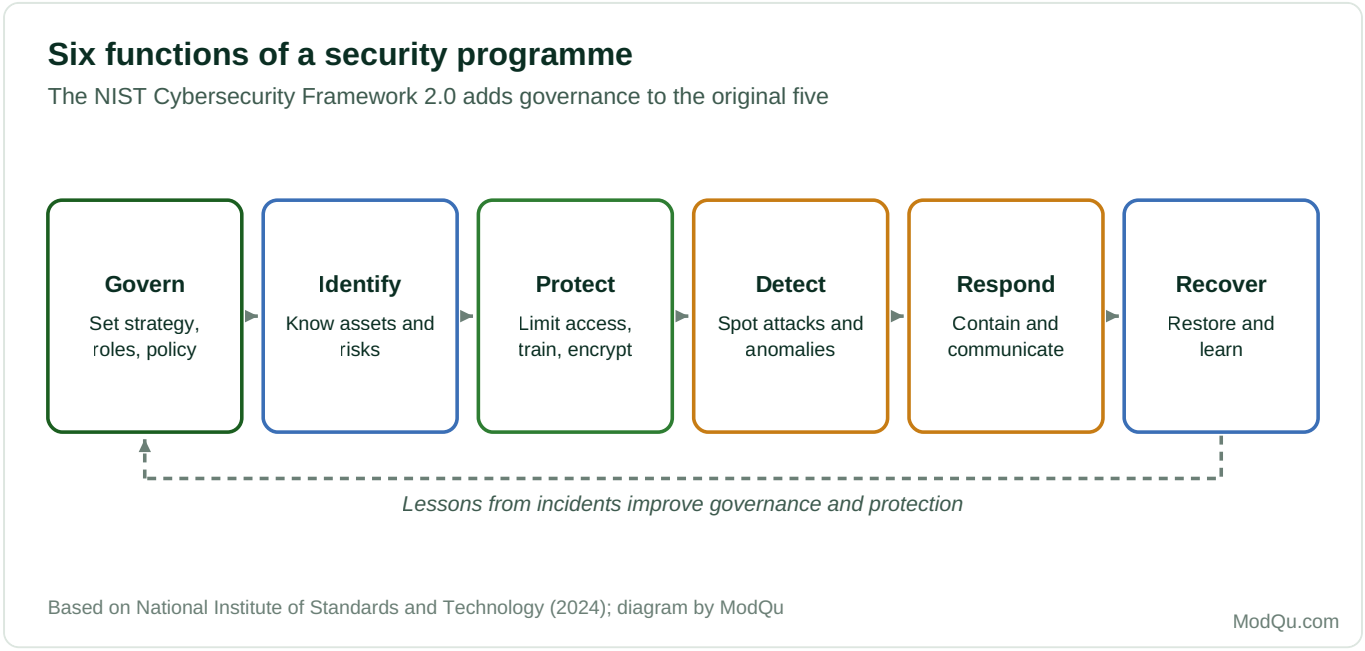


Figure 2. Six functions of a security programme. Based on National Institute of Standards and Technology (2024); diagram by ModQu.

The international standard ISO/IEC 27001 sets out requirements for an **information security management system**: a systematic, risk-based approach to managing security, including assessing risks, selecting controls, monitoring their effectiveness and improving over time (International Organization for Standardization & International Electrotechnical Commission, 2022). Many organisations seek certification to demonstrate their security to clients.

A more recent approach is **zero trust**. Traditional security assumed that users and devices inside the corporate network could be trusted. Rose et al. (2020) describe zero trust architecture, in which no user or device is trusted by default, whatever its location; every request for access is verified based on identity, device condition and context. The approach suits organisations whose staff work remotely and use cloud services, as many intelligence teams now do.

How much to spend

Security costs money, and organisations must decide how much to invest. Anderson (2001) showed that many security problems arise from misaligned incentives: the people who could best prevent a problem often do not bear its costs. Software makers, for example, may not suffer when their products are insecure. Within organisations, departments may not bear the cost of breaches they make more likely.

Gordon and Loeb (2002) developed an economic model of security investment. They showed that, under general conditions, the optimal amount to spend protecting an information asset is less than the expected loss from a breach, and that it is often not worth trying to protect the most vulnerable assets completely, because the cost of doing so rises steeply. Their model suggests investing no more than about 37% of the expected loss in protecting a given asset. While the exact figure depends on assumptions, the principle is useful: security spending should be guided by the value of what is protected and the likelihood of loss.

Practical steps for intelligence teams

Intelligence teams can apply these principles directly:

1. **Classify information.** Decide which information is public, internal, confidential or highly sensitive, and mark it accordingly.
2. **Apply need-to-know.** Give each person access only to the information their role requires. Review access when roles change and remove it promptly when people leave.
3. **Protect sources and methods.** Store details of sources separately from products, and limit who can see them.
4. **Use strong authentication.** Require multi-factor authentication for all systems holding intelligence assets.
5. **Encrypt.** Encrypt devices, sensitive files and communications, especially when working remotely or travelling.
6. **Train for social engineering.** Teach staff to recognise phishing, pretexting and unusual requests, and make it easy to report them.
7. **Make security usable.** Choose tools and rules that fit how people work, and ask staff where rules get in the way.
8. **Log and monitor.** Record access to sensitive information and review unusual patterns, such as large downloads before an employee leaves.
9. **Back up and test recovery.** Keep backups that attackers cannot reach and practise restoring from them.
10. **Plan for incidents.** Agree in advance who does what when a breach is suspected, including legal and communications steps.
11. **Check suppliers.** Data providers, research agencies and software vendors may hold or access intelligence assets; assess their security.
12. **Protect integrity.** Verify important information from more than one source, keep version histories and watch for signs of planted or altered material.

Integrity and deception

The integrity of intelligence deserves particular attention. An adversary may not want to steal an organisation's intelligence but to corrupt it: planting false information so that the organisation makes poor decisions. This can range from fake reviews and fabricated rumours to forged documents passed through apparently trustworthy channels. Protection depends on good analytic practice as much as technical controls: evaluating sources, seeking corroboration, and being alert to information that is too convenient. Security and analysis meet here.

Security during collection

Intelligence teams also need to think about security while they collect information. Research activity can reveal an organisation's interests. Repeated visits to a competitor's website from a company's own network, a burst of downloads of a particular patent class, or a series of calls to a target's suppliers can all signal what the company is investigating. Teams that handle sensitive projects should consider what their research footprint reveals and who might observe it.

This does not mean concealment or deception, which raise ethical and legal problems of their own. It means ordinary discretion: limiting the number of people who know about sensitive projects, avoiding discussion of plans in public places and on social media, using approved tools and accounts for research, and being careful about what is said to external contacts. Interviews and conversations with industry contacts are two-way exchanges; staff should be aware of what they disclose as well as what they learn.

Purchased data and outsourced research create further exposure. Contracts with research agencies and data providers should specify how client information and questions will be protected, who will have access and what happens to data at the end of the project.

Remote work and travel

Intelligence work increasingly happens outside the office, on laptops and phones, in homes, hotels and airports. Devices can be lost or stolen, public networks can be monitored, and conversations can be overheard. Basic practices reduce the risk: full-disk encryption on all devices, automatic screen locks, use of secure connections on public networks, care with printed material, and a clear procedure for reporting lost devices immediately. For travel to countries where state surveillance of business visitors is a known risk, some organisations issue clean devices that carry only the information needed for the trip.

Measuring security

Security programmes need measures, but counting blocked attacks says little about real protection. More useful measures include the time taken to remove access when people leave, the share of systems with multi-factor authentication, the proportion of staff who report simulated phishing emails, the time taken to detect and contain incidents, and the results of regular recovery tests. These measures show whether controls are working in practice, not only on paper.

A business illustration

A specialist market research firm holds confidential survey data and strategy reports for dozens of clients. An employee receives an email that appears to come from a client, asking for an updated report to be shared through a new file-sharing link. The link leads to a convincing login page that captures the employee's password. Because the firm requires multi-factor authentication, the attacker cannot log in with the stolen password alone. The attempt triggers an alert, and the security team resets the account and warns staff. A review finds that the email was well researched, referring to a real project by name, which suggests the attacker had gathered information from public sources and possibly from a previous breach at a supplier.

The firm responds by tightening its supplier security checks, running a short phishing awareness session using the real example, and limiting the project details its staff share on professional networking sites. It also reviews access rights and finds several former contractors whose accounts had not been closed. The incident causes no loss, but it shows how multiple layers of protection, technical, procedural and human, work together.

Common mistakes

- **Treating security as IT's job.** Intelligence teams know what is sensitive and how it is used; they must be part of protecting it.
- **Focusing only on outsiders.** Insiders and accidents cause a large share of losses.
- **Imposing unusable rules.** Rules that people cannot follow will be bypassed.
- **Forgetting requirements and methods.** What the team is asking, and how it gathers information, can be as revealing as its conclusions.
- **Neglecting integrity.** Protecting information from theft but not from tampering leaves decisions exposed.
- **Never testing recovery.** Backups that have never been restored may not work when needed.

Conclusion

Intelligence assets are valuable because they give an organisation an advantage, and that value makes them targets. Protecting them requires attention to confidentiality, integrity and availability; an understanding of the threats from competitors, criminals, states and insiders; and above all an understanding of people, whose errors and choices are involved in most breaches. Frameworks such as the NIST Cybersecurity Framework and ISO/IEC 27001 provide structure, and principles such as least privilege and zero trust guide design. For intelligence teams, security is not a separate concern but part of the discipline of producing intelligence that can be trusted.

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. (2001). Why information security is hard: An economic perspective. In *Proceedings of the 17th Annual Computer Security Applications Conference* (pp. 358–365). IEEE. https://doi.org/10.1109/ACSAC.2001.991552

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.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523–548. https://doi.org/10.2307/25750690

Caltagirone, S., Pendergast, A., & Betz, C. (2013). *The diamond model of intrusion analysis* (Technical Report ADA586960). Center for Cyber Intelligence Analysis and Threat Research.

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.

Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security, 5*(4), 438–457. https://doi.org/10.1145/581271.581274

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

Herley, C. (2009). So long, and no thanks for the externalities: The rational rejection of security advice by users. In *Proceedings of the 2009 New Security Paradigms Workshop* (pp. 133–144). ACM. https://doi.org/10.1145/1719030.1719050

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.

IBM. (2024). *Cost of a data breach report 2024*.

International Organization for Standardization & International Electrotechnical Commission. (2022). *Information security, cybersecurity and privacy protection: Information security management systems: Requirements* (ISO/IEC 27001:2022).

Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and other botnets. *Computer, 50*(7), 80–84. https://doi.org/10.1109/MC.2017.201

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

National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST CSWP 29). https://doi.org/10.6028/NIST.CSWP.29

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

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero trust architecture* (NIST Special Publication 800-207). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207

Saltzer, J. H., & Schroeder, M. D. (1975). The protection of information in computer systems. *Proceedings of the IEEE*, *63*(9), 1278–1308. https://doi.org/10.1109/PROC.1975.9939

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

Schneier, B. (2000). *Secrets and lies: Digital security in a networked world*. Wiley.

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

Strom, B. E., Applebaum, A., Miller, D. P., Nickels, K. C., Pennington, A. G., & Thomas, C. B. (2018). *MITRE ATT&CK: Design and philosophy* (Technical Report MP180360). The MITRE Corporation.

Tounsi, W., & Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Computers & Security*, *72*, 212–233. https://doi.org/10.1016/j.cose.2017.09.001

Verizon. (2024). *2024 data breach investigations report*.