Cybersecurity and information security: the French experience

Séminaire EURORAI de Rotterdam, 19 avril 2018

Fabrice NICOL, Chambre régionale des comptes Occitanie (Montpellier)

Cybersecurity in France : an « art of war »

Early State interventions in the fight against cybercrime

- The French State intervened through intelligence service (DST then DGSE) false flag operations, as soon as the late 80s.
- The National Cybersecurity Agency (Agence nationale de la sécurité des systèmes d'information, ANSSI), was created in July 2009.
- Not an independent administrative authority: it is attached to the General Secretariat for Defence and National Security (SGDSN)
- Surveillance strategy targeted at hacker communities, infiltrations, identification of free software leader, hiring candidates.
- Still making headlines: the hacking night of the Ministry of Defence (June 2017). Attempt to reconcile civil society values and the interests of national defence.

A belated awareness of increasing threats

- Very serious cyberattacks aimed at French institutions or businesses in 2011-2012: Presidency of the Republic, Ministry of Finances, Areva (nuclear energy leader).
- Which reinforced awareness of the threats and triggered enquiries (notably a Senate enquiry).
- Weaknesses of organisation and protection: the first public large-scale audit. Also in 2011, the Digital National Council (Conseil national du numérique) was created and a new national strategy was adopted.
- High Council for Strategic Education and Research (CSFRS): working group on *Contemporary threats and information technologies, new criminalities*. Strategy report (2012) pointing out the need for a national methodology for the evaluation and certification of information systems (IS).

Operators of Vital Importance (OVI)

- Cybersecurity advances have a military origin: article 22 of the Military Planning Act (18 Dec. 2013), following proposals of the White paper on Defence and National security of 2013. Reinforcement of the security of critical IS (IS of vital importance, SIIV).
- On 27 March 2015, two decrees were published to implement these principles:
  - decree n°2015-351 on the security of information systems of vital importance
  - decree n°2015-350 on the qualification of security products and providers of trusted services required by national defence.

This decree defines auditing standards and criteria to be met by private audit firms.

- A wide definition of protected entities that can correspond to public or semi-public entities (large public-private businesses) falling under the competence of Higher or Regional Audit Institutions. Examples:
  - French national railways (SNCF, Cour des comptes)
  - University hospitals or drinking water networks (Chambres régionales des comptes)

12 sectors of vital importance corresponding to 4 domains

SGDSN

Updating the national strategy

- The National Digital Security Strategy (Oct. 2015): essentially civilian but with military origins (article R.1132-3 of the Code of National Defence).
- Objectives : national sovereignty; fight against cybercrime; informing the general public; information security as a competitive advantage for French businesses; international actions.
- The new national cyberdefence doctrine (Dec. 2016) in the context of retaliations against terrorist attacks: an « art of war » (Le Drian).
- Preventive, coercive and proactive dimensions: retaliation and neutralisation

New challenges

- A besieged fortress: usual preventive measures (access rights privileges, firewalls, intrusion detection using signatures, compartmentalized IS) have been thwarted. Advanced persistent threats (APT) : set of stealthy and continuous computer hacking processes, often orchestrated by a person or persons targeting a specific entity (Pernet 2014)
- Why?
  1. Growing number of networks and servers.
  2. Widespread use of encryption and trace obfuscation (Tor, VPN in fiscal heavens) and of malicious code (hacking as an ultimate discipline of expertise)
  3. The failure to attribute attacks and to legally repress them.

Ineffective laws

"Whether in Europe, the United States, Russia, China, Africa, or Brazil, few cases of 'cyber-crimes' are effectively treated by the judicial system, and much less have been sanctioned. The mechanisms of judicial co-operation are very often ineffective in the areas of cybercrime, not through a lack of talent,—as State forces usually have decisive talents in this area—but by the unworkable nature of the technical cooperation on cybercrime." (Baumard 2017, p.39, Fleck 2012, Kenneth 2010)

- Diverging interpretations of the Council of Europe Convention on cybercrime, ratified by few countries (less than 60 in March 2018).
- How to assess the way audited entities take up the new challenges? Their responsibilities in case of damages caused by a cyberattack?

Extending the security strategy

- The European directive EU n°2016/1148 Network and Information Security (NIS, 6 July 2016) aims to achieve a high common level of security for EU networks and information systems. The French Act passed on 26 Feb. 2018 transposed this directive.
- It reinforces protection against more frequent and sophisticated cyberattacks which *« can now very seriously impact the physical world »* (ANSSI).
- It extends the strategy to other non-OVI entities in the public and private sectors, which remain very vulnerable to cyberattacks like WannaCry : **operators of essential services**.
- As a consequence, new entities fall under the competence of Higher or Regional Audit Institutions

Audit institutions as stakeholders

- The law provides for security and certification rules **(= audit themes**) pertaining to:

  « 1° The governance of the security of networks and information systems
  2° The protection of networks and information systems
  3° The defence of networks and information systems
  4° The resilience of activities.
  The rules stated in the first paragraph can notably provide that operators use hardware, software or computer services certified for security. » (article 6 loi 27 février 2018)

- ANSSI is recognised as a specialised Audit Institution:

  « Audits will be performed on records and on the spot by the national cybersecurity authority referred to in article L. 2321-1 of the Code of Defence or by service providers qualified by the Prime Minister » (Art. 8)

- New competition for the institutions traditionally in charge of controlling/auditing accounts and management?

Audit and control of information security:
a French perspective

Assessing the financial performance of countermeasures

- Reinforcing countermeasures is necessary (intrusion detection). Three categories of tools:
  - Well-known methods based on detecting intrusion signatures (antivirus)
  - Behavioural methods (analysing how information systems react to cyberattacks)
  - Artificial intelligence / Deep learning
- Measure costs are increasing: a balancing act between effectiveness and efficiency. The balance point depends on incurred costs after a cyberattack, which cannot been reliably anticipated.
- Costs are shifting away from hardware to software and human resources.

Assessing audit methods used in France

- The EBIOS method (ANSSI) : context, anticipated events, threat scenarios, risks, security measures. Compatible with standards ISO 13335 (GMITS), ISO 15408 (common criteria) and ISO 17799.
- Clear, exhaustive et flexible but no immediate solutions: essentially a diagnostic method.
- The MEHARI 2010 method elaborated by CLUSIF (French Information Security Club, independent association open to all businesses and communities) now developed in Quebec (CLUSIQ), compatible with ISO 27005:2009 standard. Can also be used in the context of Information security management systems (ISO 27001:2005). Several levels. PRO version for SMEs. Free.
- French Higher and Regional Audit Institutions: no specialised methods for cybersecurity audits to date. However a guide on the audit of information systems has been made available. (Centre d'appui métier of the Cour des comptes).

High audit costs

- An oligopolistic market: few private firms have been certified (about 25): Airbus Defense and Space, Bull, CGI, CS, Ernst and Young, Steria, Orange,PWCA, Sogeti, Thales. 10 % are SME startups.

- High costs: €60,000 on average (Baumard 2017) for a basic cybersecurity audit.

- These audit costs can only occasionally be afforded by French Audit Institutions.

Some priorities in the context of limited resources

- Audit institutions have a competitive edge: the experience of a systemic, global approach of auditing and control.
- Computer techniques are only part of a global strategy and should implement coherent policies: strategy, budget, human resources, internal control, processes, legal compliance, modernisation of tools, monitoring technological advances.
- All international audit standards comprise a functional module dealing with the above domains and the CISO's role (Chief Information Systems Officer).

The challenge of assessment audits

- Threat audits and validation audits: to date, ANSSI and certified service providers alone are in a position to perform these types of audits.
- Assessment audits - French Audit Institutions have a role to play and can develop expertise:
  - assessing whether measures comply with regulations and standards
  - mapping responses to identified threats
  - assessing effectiveness and efficiency of these responses
  - assessing the security posture (both strategic and tactical)
- Auditing personal data security is a particular case that can be technically and financially handled by French Audit Institutions.

Auditing personal data security

- A French tradition (Computing and Freedom Act, 6 Jan. 1978), which will be updated when the *General Data Protection Regulation (GDPR)* comes into force in May 2018.
- The French National commission for computing and freedom (CNIL) proposes practical tools (PIA software). It is replacing labelling with certification.
- It is promoting **action plans** **that can also be used for audits**: steering procedures/committees, mappings, setting priorities, identifying risks, internal processes, documenting procedures and compliance with standards and regulations.

Professional uses of personal data by French Audit Institutions

- French Audit Institutions use payroll databases (DB) for computerised mass processing.
- Depending on levels and entities:
  - The State payroll DB is anonymised and encrypted. DB fields can on occasion been deciphered by decision of the Ministry of Finances.
  - Payroll DB for some State institutions and all local government bodies are nominative and not encrypted, mainly under XML format, and preserved between 4 and 6 years, sometimes more.
  - Software like Xemelios, CDGD, ORC, Altaïr make it possible to obtain or mass process data up to 20 million lines of payroll DB per year for the City of Paris.
- Compliance with GDPR is uncertain in the latter case.

Precautionary measures to be taken (I)

- *Recital 45 - 'Where processing is carried out in accordance with a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority, (…) that law could specify the general conditions of this Regulation governing the lawfulness of personal data processing, establish specifications for determining the controller, the type of personal data which are subject to the processing, the data subjects concerned, the entities to which the personal data may be disclosed, the purpose limitations,* ***the storage period*** *and other measures to ensure lawful and fair processing.'*

- To date, no standard fixing how long payroll DB will be preserved by the Chambres Régionales des Comptes and some State bodies falling under the competence of the Cour des comptes.

Precautionary measures to be taken (II)

- *Recital 97 – ‘ Where the processing is carried out by a public authority, except for courts or independent judicial authorities **when acting in their judicial capacity**,(…), or where the core activities of the controller or the processor consist of processing on a large scale of special categories of personal data and data relating to criminal convictions and offences, **a person with expert knowledge of data protection law and practices** should assist the controller or processor to monitor internal compliance with this Regulation. In the private sector, the core activities of a controller relate to its primary activities and do not relate to the processing of personal data as ancillary activities. The necessary level of expert knowledge should be determined in particular according to the data processing operations carried out and the protection required for the personal data processed by the controller or the processor. Such **data protection officers**, whether or not they are an employee of the controller, should be in a position to perform their duties and tasks in an independent manner.’*
- French Audit Institutions using payroll DB for mass data processing should therefore, in principle, appoint a DPO (*Data protection officer*) in charge of data used in administrative procedures.
- Examples in France: management control (contrôle de gestion); budgetary control (contrôle budgétaire) by a Chambre régionale des comptes.
- Need to update professional standards and the regulations related to Audit Institutions?

References

Baumard, Philippe (2017) *Cybersecurity in France*, Springer Briefs in Cybersecurity, Springer

Donaldson, Scott E.; Siegel, Stanley G. ; Williams, Chris K. and Aslam, Abdul (2015) Enterprise Cybersecurity: How to Build a Successful Cyberdefense Program Against Advanced Threats, Springer Science, Apress.

Fleck D (2012) *Searching for international rules applicable to cyber warfare—a critical first assessment of the New Tallinn manual*. Int J Conflict Secur Law 18(2):331–35

Kenneth G (2010) *The challenge of cyber attack deterrence*. Comput Law Secur Rev 26(3):298–303

Pernet, Cédric (2014) *Sécurité et espionnage informatique : Connaissance de la menace APT (Advanced Persistent Threat) et du cyberespionnage*, Eyrolles