–CYBERSECURITY IN BRITTANY: FOCUS ON EXPERTISE–

LES ÉTUDES DE L'EMPLOI CADRE

N°2017-25

JUNE 2017

SUMMARY

In a social, technological and regulatory environment that is constantly developing, cybersecurity is becoming an ever more important issue, in particular with regard to executive employment. 90% of IT specialists questioned by Apec considered that businesses are poorly prepared in this area. There is therefore a very great requirement for the skills and expertise needed to rise to this challenge. Endowed with a genuine cybersecurity infrastructure, Brittany plays an important role in this field. Although the requirements at job level are extremely technical, more intuitive skills are also crucial. To facilitate recruitment by business, it is particularly important to ensure ongoing training. Indeed, 85% of IT specialists in Brittany would like to improve their cybersecurity skills.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PRÉFET DE LA RÉGION BRETAGNE

Région BRETAGNE

BRETAGNE DÉVELOPPEMENT INNOVATION

PÔLE D'EXCELLENCE CYBER

Apec

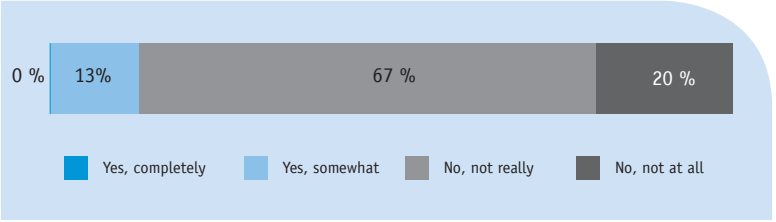
CYBERSECURITY: A KEY ISSUE AND A CHALLENGE

Information systems are at risk from a range of threats: data theft, industrial espionage, hijacking of machines or production lines, fraud or identity theft, ransom demands. For businesses, the financial consequences of cyber-attacks are severe: 1.5 billion euros of financial loss in the year 2016 alone (annual survey by PwC[1]). Whatever its size, the risk that a company will be the object of an attack is growing. This growing risk is also forcing businesses to take measures to protect themselves. There is a general responsibility (including under criminal law) for businesses to ensure the security of their IT systems. What is more, technological developments (in the interdisciplinary domains of cloud computing, connected objects, big data, etc.) and IT practices (digital nomadism, social networks, etc) all bring with them significant risks in terms of IT security. For businesses, cybersecurity simultaneously constitutes a vital issue, a regulatory obligation and a strategic positioning. It can therefore be defined as "*a desired state for an information system that allows it to withstand events arising in cyberspace that might compromise the availability, integrity or confidentiality of stored, processed or transferred data and the associated services that these systems offer or make accessible*"[2].

Even though a certain level of awareness has emerged in recent years regarding the importance of cybersecurity, businesses still lack maturity concerning this subject. They acknowledge this themselves: only 53% of industry managers consider that their companies are properly prepared for the questions raised by cybersecurity[3]. The IT specialists questioned by Apec were even more critical: 86% of them considered that businesses in general are not properly prepared when it comes to the subject of cybersecurity **(Figure 1)**. They were also almost unanimous (85%) in thinking that employees are not sufficiently familiar with good IT security practices. It therefore seems that a great deal of work still has to be done in order to instil a cybersecurity culture in businesses.

1. PwC, The Global State of Information Security® Survey 2017.
2. Definition issued by Anssi (Agence nationale de la sécurité des systèmes d'information / National agency for the security of information systems) cited in the Technical reference document (version 4.1.1) published by the *Pôle d'excellence cyber*.
3. Usine Nouvelle – Orange Business Services survey conducted in November 2016 among 347 industry directors.

– Figure 1–
Nowadays, we hear a lot about cybersecurity. Do you think that businesses in general are well prepared?



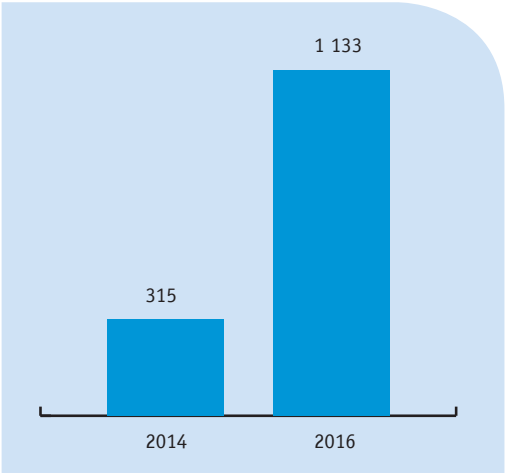
Source : Apec, 2017. Survey conducted among IT specialists logged on to Apec.fr during the last 12 months.

CYBERSECURITY: AN EMPLOYMENT OPPORTUNITY

In a context in which businesses are extremely concerned about IT security, all the available studies point to a considerable growth in jobs dedicated to cybersecurity[4]. The growth in the number of job vacancies published by Apec for executive cybersecurity positions also testifies to this trend. The number of job vacancies published by Apec for cybersecurity-related positions grew by a factor of 4 between 2014 and 2016, increasing from 315 to 1,133 **(Figure 2)**.

4. See, for example, Pipame, *Le secteur industriel français de cybersécurité (The French industrial cybersecurity sector)*, January 2016.

– Figure 2–
Job vacancies published by Apec for cybersecurity-related positions



Source : Apec, 2017

A cybersecurity job market is therefore beginning to take shape and involves various types of actors.

1. **Businesses that make use of cybersecurity services**. Business of all sizes and from all sectors want to boost their capabilities in this area either through direct recruitment or by buying in external expertise. The so-called "operators of vital importance" (OVI) are extremely active. These are companies or state services active in sectors of particular strategic importance (finance, energy, transport, health, etc.).
2. **Service providers**. Large companies providing consulting or IT services have developed lines of business that specifically target cybersecurity. In particular, they provide their expertise in the form of security audits, risk analyses, etc. Start-ups are also extremely active and offer highly specialized service activities as well as product development activities (software, secure data exchange platforms, security packages, etc.).
3. **The defence sector**. Companies specializing in the defence sector (Thales, Airbus CyberSecurity, etc.) have also developed a high level of expertise in the cybersecurity field. The French Ministry for Armed Forces itself is one of the leading recruiters of cybersecurity specialists.

Cybersecurity is therefore a driver of IT-related employment and the field is expected to continue developing in the years to come. The IT specialists questioned are convinced of this. When asked to judge on a scale of 0 to 10 whether cybersecurity is currently a growth sector for employment, 29% gave a rating of 8, 9 or 10. However, when asked to rate the situation in 3 to 5 years from now, the proportion rose to 69% **(Table 1)**.

– Table 1–

On a scale from 0 to 10, would you say that cybersecurity is a growth sector for employment (0 not at all, 10 very much so) ?

	At present	In 3 to 5 years
10	9%	22%
9	5%	22%
8	15%	25%
7	19%	14%
6	19%	7%
5	13%	6%
4	7%	2%
3	8%	1%
2	4%	1%
1	1%	0%
0	0%	0%
average score	**6**	**8**

Source : Apec, 2017. Survey conducted among IT specialists logged on to Apec.fr during the last 12 months.

CYBERSECURITY IN BRITTANY: ACKNOWLEDGED LEADERSHIP

Brittany has a genuine ecosystem that is beneficial for the further growth of the cybersecurity sector. What is more, outside of Île-de-France, it is the only French region to possess a rich and complex infrastructure[5], benefiting from the long-standing presence of state organisations (DGA-MI: Direction générale de l'Armement – Maîtrise de l'information (DGA Information Superiority, an establishment of the French Defence procurement agency), École des transmissions (a military academy), etc.), the presence of leading private actors in this field, and a high density of civil and military training and research centres. Thus in 2014, at the initiative of the French Ministry for Armed Forces and the Brittany Region, the *Pôle d'excellence cyber* was founded in Brittany and has the task of supporting the nationwide development of the cybersecurity and cyber-defence sector through its three indissociable missions of training, research and industrial development. As far as Brittany itself is concerned, the various stakeholders again reflect these three areas of activity:

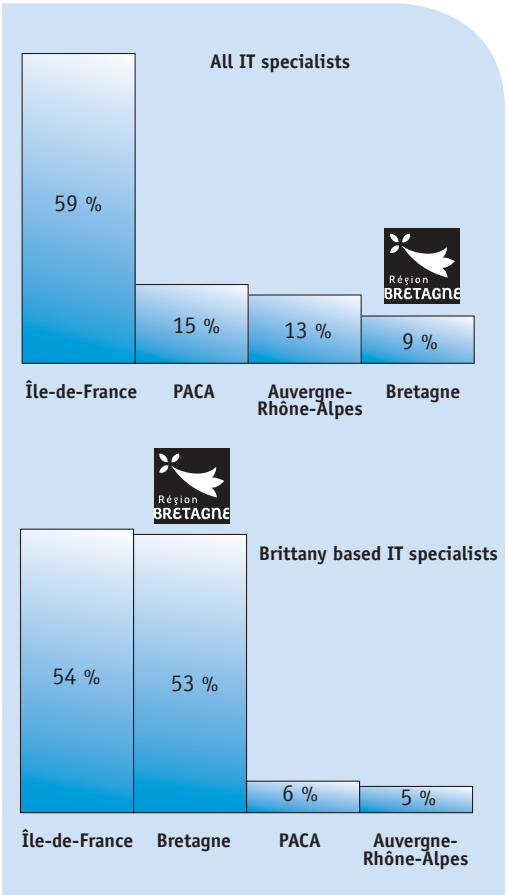
- **Training**: some ten or so higher education establishments offer basic and ongoing training in cybersecurity, including a number of top-level courses.
- **Research**: in Brittany, 200 researchers are employed in the field of cybersecurity in high-level research centres.

5. Usine Nouvelle, *Cybersécurité : les 40 sites stratégiques (Cybersecurity: the 40 strategic sites)*, issue 3452, 21st January 2016.

• **Economic development**: a number of large groups are present in the region, together with a wealth of innovative SMEs and midsize businesses.

Brittany's outstanding expertise in the field of cybersecurity is widely recognized. Thus the Brittany-based IT experts questioned by Apec cite Brittany as being in second position among the French regions and consider it to be particularly advanced in the field of cybersecurity, occupying a position just behind Île-de-France. The actions undertaken by the Brittany Region with regard to cybersecurity therefore resonate with the population of IT specialists that live there. This reputation extends beyond the region's borders: French IT experts rank Brittany in 4th place among the regions that are most highly advanced in the field of cybersecurity, ahead of regions such as Occitanie or Hauts-de-France **(Figure 3)**.

– Figure 3 –
The most highly advanced regions in terms of cybersecurity according to IT specialists (two answers possible)

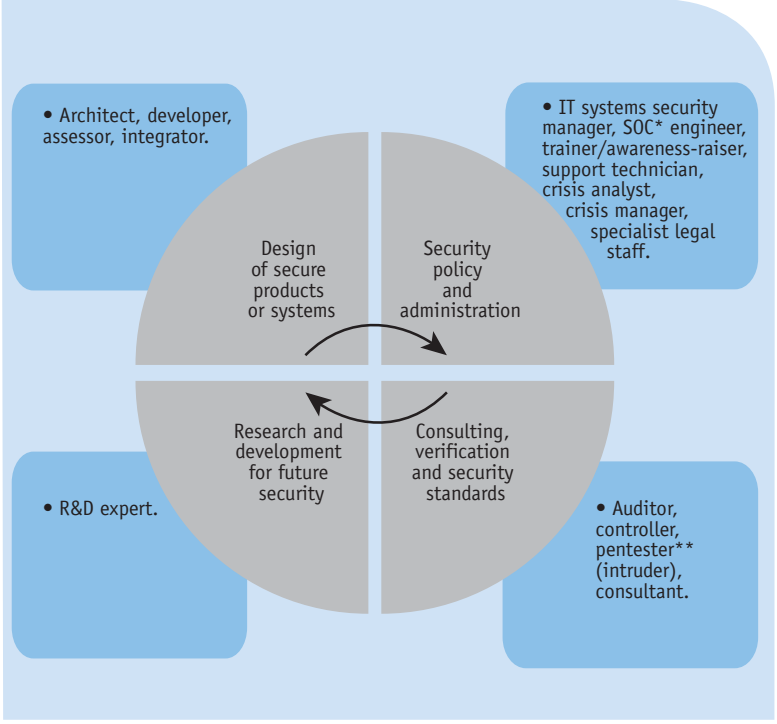


Source : Apec, 2017. Survey conducted among IT specialists logged on to Apec.fr during the last 12 months.

HIGHLY SOUGHT-AFTER SKILLS IN A DIFFICULT ENVIRONMENT

According to the reference material relating to cybersecurity drawn up by the Pôle d'excellence cyber, almost all jobs in this field are of executive level. Highly developed technical skills are demanded in all these positions **(Figure 4)**: evaluation of components or software, design of secure architectures, detection of penetration tests, modelling of threats and attacks, anti-virus design, cryptography, etc. Beyond their technical know-how, applicants are also expected to possess so-called behavioural skills. Curiosity, versatility, interpersonal skills, an ethical approach and a sense of service are cited by recruiters as personal capabilities that are needed in the professional environment of future cybersecurity specialists and that are therefore crucial for anyone working in the cybersecurity field.

– Figure 4–
Jobs in the cybersecurity environment



Source : Apec, 2017. Based on the work of the Reference documentation group at the Pôle d'excellence cyber.
* The SOC (security operation centre) is a centre for security supervision and administration. It collects information (login journals for example), detects anomalies and proposes responses.
** Pentesters specialize in penetration tests (also referred to as "pentests"). During audits, they penetrate IT systems in order to detect security loopholes.

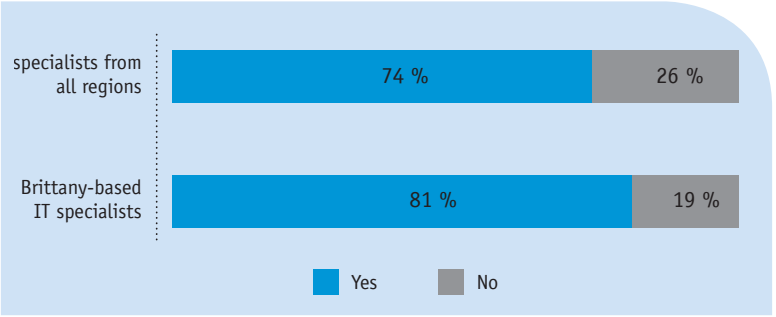
Brittany-based businesses agree that recruitment difficulties exist for the majority of these jobs. The shortfall is particularly striking in the case of cybersecurity consultants, security architects, security developers, security auditors. Despite these difficulties, Brittany-based companies find it possible to hire by adapting their recruitment methods to the target market. Networks of personal contacts and cooperative strategies are very frequently mobilized. Their location in Brittany also seems to be a key asset for the interviewed businesses.

Although tensions exist in the cybersecurity sector of the IT employment market in Brittany, they are nevertheless limited compared to the Paris region. Executives in Brittany are very attached to their region and have little desire to relocate to other regions, thus restricting staff turn-over. The quality of life in the region also helps attract executives from elsewhere, in particular from the Paris area. Thus, among IT specialists prepared to change region when changing job, 24% name Brittany as a possible destination, making it the most attractive region alongside Nouvelle-Aquitaine and Paca (Provence - Alpes - Côte d'Azur).

A SECTOR CONSIDERED VERY ATTRACTIVE BY IT SPECIALISTS

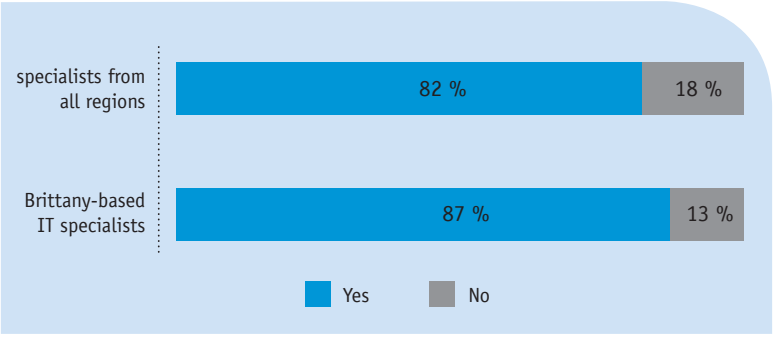
Businesses can also benefit from the attractiveness of the cybersecurity field for IT specialists. Indeed, 78% of IT specialists would definitely be interested in working in the cybersecurity field **(Figure 5)**. This proportion increases to 82% for Brittany-based IT specialists. And, more generally, 83% of them want to develop their cybersecurity skills (85% in Brittany) **(Figure 6)**. It is worth noting that there is a considerable difference in opinion between men and women regarding these questions even though the results are very similar on the other points. In effect, whereas 79% of male IT specialists say that they would definitely be interested in working in the cybersecurity field, the same is true of only 54% of the women, i.e. 25 points fewer. Similarly, a smaller proportion of women than men want to develop their cybersecurity skills: 67% compared to 85%. The ability of cybersecurity to attract women is therefore problematic and this should be interpreted as a warning sign for the future.

– Figure 5–
Would you definitely be interested in working in the cybersecurity field?



Source : Apec, 2017. Survey conducted among IT specialists logged on to Apec.fr during the last 12 months.

– Figure 6–
Would you like to develop your cybersecurity skills?



Source : Apec, 2017. Survey conducted among IT specialists logged on to Apec.fr during the last 12 months.

In addition, the task of building up expertise could be a difficult one because fewer than 40% of the IT specialists questioned said that they possessed technical skills in the area of cybersecurity. And of those, only a small proportion thought that they had a very good level of knowledge when asked to rate themselves on the various subjects on a scale of 0 to 10 (design of secure architectures, penetration detection, security tests, cryptography, etc.). The IT specialists rated themselves higher than 6 out of 10 on only one of the 11 fields of technical expertise in cybersecurity about which they were questioned (raising user awareness). For 9 out of the 11 fields, the average grade was less than or equal to 5.
This clearly raises questions relating to the development of the cybersecurity skills of the IT specialists currently present in the market.

CONSIDERABLE EXPECTATIONS WITH REGARD TO ONGOING TRAINING

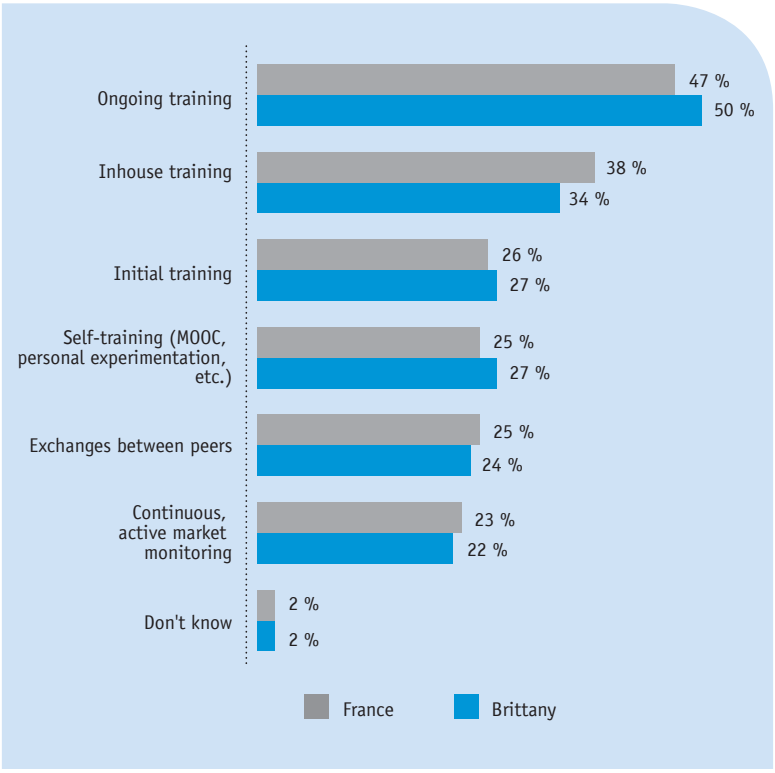
There is a relatively robust offer in the field of cybersecurity training, in particular in Brittany. Specific training courses continue to be developed both at university and major academy level. However, it should be noted that companies are not only looking for junior staff. Many of the professions involved in cybersecurity demand experience. This is particularly true of jobs that contribute to the definition and administration of cybersecurity policy in industry. However, it also applies to consultants, auditors and architects. Thus an examination of the cybersecurity positions published on the Apec site shows that the great majority of the posts are not available to beginners and young graduates.

A significant effort is therefore expected in terms of ongoing training, not only to make it possible to adapt the skills of specialists to methods and practices that are constantly evolving, but also to boost the expertise of existing executives who have received no initial cybersecurity training. The adoption of ongoing training measures would also make it possible to make unemployed IT specialists more attractive on the labour market and to reposition them in businesses that are looking to recruit. And this is all the more so given the very high level of demand on the part of IT specialists already present on the market. Among the IT specialists stating that they want to develop their cybersecurity skills, 9 out of 10 would need either ongoing training (including a resumption of studies) or internal training in their company **(Figure 7)**.

The desire for ongoing training on the part of IT specialists, in particular in Brittany, raises the question of the type of training that needs to be developed in order to meet the stated wishes. The different routes into the cybersecurity-related professions are not always clearly identified either by the executives in question or by the companies themselves. There is a need to make the possible career paths and the training required in order to work in the cybersecurity field clearer, in particular in existing or future job descriptions.

– Figure 7–

What do you most need in order to develop your cybersecurity skills (maximum of 2 responses)?



Source : Apec, 2017. Survey conducted among IT specialists logged on to Apec.fr during the last 12 months.

AN ACTION PLAN TO ENCOURAGE THE DEVELOPMENT OF CYBERSECURITY SKILLS IN BRITTANY

This study has resulted in an action plan which will be implemented this year by the Apec delegation in Brittany in collaboration with the partners to the study. Apec is therefore committed to undertaking a range of concrete actions in three areas: to develop knowledge of the professions available in the cybersecurity field and to promote these professions, to work with cybersecurity companies in Brittany in order to meet their needs (recruitment, ensuring employee loyalty, etc.), to support executives and young graduates in Brittany looking to access opportunities or change focus within the cybersecurity sector (consulting, guidance, organisation of events, etc.). Some of these actions will continue beyond 2017. ●

–METHODOLOGY–

This study was conducted by Apec's study and research department and its regional delegation on behalf of the Brittany Region and the State within the framework of a call for projects for action studies provided for in the State-Region planning contract. The *Pôle d'excellence cyber* and *Bretagne Développement Innovation* contributed to this undertaking and were represented on the steering committee.

The study took place in two phases:

– A qualitative survey in the form of individual interviews and working groups among some thirty companies, primarily in Brittany, that were seeking cybersecurity skills. A number of experts were also questioned.

– A quantitative online survey of 1,200 IT specialists identified from Apec's records, including 600 Brittany-based. 85% of these IT specialists were employed at the time of the survey. Nine out of ten were executives (in their current position or their last job). Following adjustment, the questioned population is representative of the IT specialists registered with Apec.fr over the last 12 months both by age and region. This is a population in search of work or monitoring developments in the job market, thus making their view of the market and their wishes for personal development even more interesting. This study has resulted in a concrete action plan which will be implemented by the Apec delegation to Brittany and the partners to the study.

ISBN 978- 2-7336-1110-4
JUIN 2017

This study was undertaken by Apec's studies and research department in association with the Apec regional delegation to Brittany.
Supervision of study : Gaël Bouron.
Analysis and editorial work : Caroline Legrand, Sophie Roux.
Head of study : Maïmouna Fossorier.
Head of department : Pierre Lamblin.
Apec regional delegate for Brittany : Anne Savatier.

ASSOCIATION POUR L'EMPLOI DES CADRES
51 BOULEVARD BRUNE
75689 PARIS CEDEX 14

POUR CONTACTER L'APEC
0 809 361 212
Service gratuit
+ prix appel
DU LUNDI AU VENDREDI
DE 9H À 19H

www.apec.fr

EDOBSA0236–S–05.17