Sectoral Analysis

April 2024

CROSS CHANNEL INSTITUTE

for the promotion of Franco - British sustainable prosperity

Cybersecurity Insights

Building Trust in the Franco-British Relationship

FRANCO BRITISH *Chamber*

Table of Contents

Introduction

Olivier Campenon,
Chairman of the Cross-Channel Institute,
CEO, Group Lefebvre

This white paper, entitled **"Cybersecurity Insights: Building Trust in Franco-British Relationship"**, is a sectoral analysis commissioned by the Cross-Channel Institute, the Franco-British Chamber's apolitical and independent think tank. The study delves into the challenges confronting businesses within the cybersecurity landscape of 2024, with focus areas including the era of the polycrisis, AI-related threats, ransomware and multi-extortion, cloud adoption and supply chain risk, and the intensifying regulations.

The paper provides invaluable insights into how organisations can brace themselves against such threats and foster resilience. In addition, the paper scrutinizes regulatory frameworks and compliance hurdles that organisations operating in both nations are faced with. It also highlights the continuing cross-border collaboration and dialogue on cyber issues. Despite certain disparities and divergences, the paper asserts that a mutual trajectory and a shared ambition of safeguarding and unlocking value by fostering a more secure cyberspace for trade are evident.

Furthermore, this research pays particular attention to the concept of cybersecurity governance. This process—the control and direction of an organisation's cybersecurity activities—is elaborated upon. The paper discusses the significance of cybersecurity governance to business resilience, details some of the key features of effective governance, and outlines the present approaches and challenges in both the UK and France. It also looks at future trends and best practices in cybersecurity governance, such as the ISO/IEC 27001 standard, the UK Cyber Governance Code of Practice, and the ramifications of AI.

To conclude, while this document does not claim to be comprehensive, it aims to serve as a reliable resource that aids organisations in implementing and sustainably maintaining effective cybersecurity measures—particularly for entities engaged in trade between the UK and France.

Cybersecurity: A Strategic Cross-Channel Partnership

French Ministry for Europe and Foreign Affairs

Throughout the 120 years of Entente cordiale, France and the United Kingdom have efficiently worked together on the traditional strategic domains: land, sea, air and space. Moreover, the increasing importance of cyberspace for the security and prosperity of our societies has led our two countries to invest in cybersecurity in order to harness opportunities and overcome challenges generated by the digital age. In a more complex, interconnected and volatile world, cybersecurity has become a key dimension of the Franco-British relationship. In this ever-evolving context, our two countries can build on a long-standing strategic proximity engraved in the Entente cordiale and the 2010 Lancaster House treaties.

In March 2023, the 36th France – United Kingdom Leaders' Summit reaffirmed our longstanding friendship and partnership and sealed a shared vision for our common future, including in the cyber domain. Beyond this year's celebrations of our close diplomatic ties, there is no doubt that 2024 is and will be a cyber year between our two countries. The existence of common interests was illustrated no later than February 6th with the formal launch of the Pall Mall Process, a joint international initiative to tackle the proliferation and irresponsible use of commercial cyber intrusion capabilities, in the historical venue of Lancaster House in London.

The annual France – United Kingdom cyber dialogue benefited from a new impetus in 2023. This format allows us to take stock of our cooperation and build a common vision for the future of our respective and joint projects. On both sides of the Channel, we share a commitment to uphold the normative framework for responsible State behavior in cyberspace based on international law, and to promote a free, open, inclusive, non-fragmented and secure cyberspace. In this endeavour, we are strengthening our coordination at the United Nations. At the bilateral level, we regularly exchange on the evolution of the cyber threat landscape, highlighting our common understanding of specific threats, including the cyber intrusion market, which could be used for offensive purposes. Cooperation between our two countries is also key to ensure the cybersecurity of large events, especially as the Olympic and Paralympic Games will take place in Paris in a few months.

Over the years, France and the United Kingdom have also developed their specific models of governance which continue to be a source of mutual inspiration and an element of interest for companies eager to navigate both markets.

As a member of the European single market, France is an active EU Member State in the elaboration of the Union's regulations (NIS2 Directive, Cyber Resilience Act, Cybersecurity Act, Cyber Solidarity Act) and strategies (EU Cybersecurity Strategy). By demanding an increased level of cybersecurity for institutions, critical infrastructures and products across the EU, these regulations both ensure our common protection and offer market opportunities to the cyber sector. Additionally, cybersecurity is one of the European Commission's priorities in its investments for the future of the Union: the EU's long-term budget, coupled with NextGenerationEU, has included additional investments in cybersecurity, as well as various investment funding programmes (Digital Europe Programme, InvestEU), and the support for research and innovation in the field of cybersecurity is led by Horizon Europe.

In this environment, France remained Europe's number one destination for foreign direct investment projects in 2023 according to EY Attractiveness Report Europe, thus confirming the attractiveness of French innovation and business environment. The "France 2030" investment plan contains a €1 billion national acceleration strategy for cybersecurity to develop sovereign and innovative cybersecurity solutions, reinforce synergies between players in the industry, support demand by raising awareness on cybersecurity, and train a new cybersecurity workforce.

The thriving French cybersecurity ecosystem is mirrored by the United Kingdom's, as the NCSC assesses the British cybersecurity sector's contribution to the economy at £10 billion. Thanks to leading cyber expertise, the two markets are growing fast. In this ever-evolving and competitive field, we encourage private actors to make the best of the existing opportunities and create new ones. In this endeavour, we believe that France and the United Kingdom have everything to gain in encouraging the development of leading companies and organisations to build trust and security in cyberspace and across our societies. *Vive l'Entente cordiale !*

French Ministry for Europe and Foreign Affairs

In an increasingly uncertain security environment, large companies need to equip themselves with systems for alerting, restoring and cleaning up their information systems. The European DORA regulation already imposes a certain number of requirements on large companies, and we can imagine that these systems will be extended across the Channel. Consequently, Infotel has developed Cyber software and services for its customers in both France and the UK.

Cleaning and Resilience

Who wants to break into an empty house?

Among the solutions developed, the **Deepeo** software enables sensitive and personal data to be cleansed. It can also be used to anonymise data in production within the IT system.

Cyberattacks are always a possibility.

As banking systems are particularly vulnerable to cyber-risks, Infotel distributes and installs a **monitoring system** for large banking and insurance information systems. To guarantee the resilience of our businesses, it is vital to detect attacks and their targets as quickly as possible, so that systems can be restored, quickly, to their original state.

Arnaud Siminski

Business Unit Director, INFOTEL

British Embassy in Paris

The British Embassy in Paris is pleased to support the work of the Cross-Channel Institute, the Franco-British Chamber's independent think tank, during an important year for UK-France relations. 2024 marks the 120th anniversary of the Entente Cordiale, an opportunity for both countries to celebrate our historic friendship and global partnership.

Over the past year, the UK-France bilateral trading relationship has reached over £103 billion, back to nominal levels last seen in 2019. Both governments are committed to furthering trade and investment ties between the UK and France to protect our economic security and drive future prosperity. According to the EY Attractiveness Survey 2023, France and the UK were the two leading foreign direct investment destinations in Europe. The UK once again ranked highest in Europe for the number of new (greenfield) FDI projects and continued to deliver more total jobs and jobs per project than France and Germany.

In March 2023, the UK Government launched its Science and Technology Framework. This framework, backed by our Prime Minister Rishi Sunak, has placed the UK at the forefront of emerging technologies including artificial intelligence, quantum technologies, semi-conductors, future telecoms and cybersecurity.

At a bilateral level, the UK is committed to working with France to develop our science, technology and cyber cooperation:

AI Safety Summit: In November 2023, the UK hosted the first AI Safety Summit, which was convened by the UK to identify next steps for the safe development of frontier AI through the signing of the Bletchley Declaration. France will host the next in-person AI Safety Summit, and we look forward to working closely with the French Government to drive forward this important agenda.

Science and Technology Joint Committee: On 29th February, the UK and France held its first Science, Technology and Innovation Joint Committee in London, where £800,000 of joint funding was announced to support more UK-French bids for research funding, like Horizon Europe.

Cyber Dialogue: At the UK-France Leaders' Summit in March 2023, the UK and France agreed to give new impetus to the UK-France Cyber Dialogue. This reaffirmed our joint commitment to uphold a free, open, inclusive, non-fragmented and secure cyberspace. The UK and France agreed to tackle the proliferation and irresponsible use of commercial cyber intrusion capabilities.

Commercial Proliferation: On 6th February 2024, the UK and France brought together an international community in London to discuss growing concerns around the proliferation and irresponsible use of commercial cyber intrusion capabilities. The conference launched the Pall Mall Process, a new international initiative to explore policy options and new practices to address this shared threat.

Paris 2024 Olympic and Paralympic Games: The UK and French governments and industry have cooperated closely ahead of the Paris 2024 Olympic and Paralympic Games. It has been important to share best practice in terms of event security, building on the UK's experience of organising the London 2012 Olympic and Paralympic Games and the Birmingham 2022 Commonwealth Games.

Looking beyond the government-to-government cooperation, the technology and digital sectors are already an intrinsic part of the UK-France trade and investment relationship. The UK tech sector is valued at over $1 trillion – third in the world behind the US and China – and we're home to over 140 unicorns. At last count, telecommunications, computer and IT services represented the third biggest UK services export to France at £2.9 billion over the past year. Artificial intelligence will be a key driver in this sector, and the UK Government is committed to working with companies to accelerate its adoption. That's why we have launched the AI Opportunities Forum, co-chaired by Michelle Donelan, Secretary of State for Science, Technology and Innovation and Lord Franck Petitgas, the Prime Minister's Special Adviser on Business and Investment, to maintain a dialogue with the private sector on harnessing the potential of AI in the economy.

Of course, cybersecurity is critical to a thriving technology sector. The UK boasts a developed cybersecurity ecosystem, with almost 2,000 cyber companies and over 50,000 people employed across the industry. There are significant UK companies with operations in France who focus a large proportion of their activity on cyber. For example, British Telecoms (BT) in France supports companies to manage cyber-risk through its Security Operations Centre in Paris. Moreover, in recent years Darktrace, a UK cyber tech company, has successfully expanded to the French market with an office in Paris. Darktrace, established in 2013, has grown rapidly to reach unicorn status with a valuation of £3 billion. These cyber companies not only play a pivotal role in protecting infrastructure and industry, but also are an important contributor to UK exports.

The British Embassy in Paris has an exciting science and technology agenda in 2024. On 21st March, we held a UK-France "Bienvenue au Royaume des Audacieux" tech showcase in the Ambassador's Residence. Looking ahead, the UK will be making a return to VivaTech in May with a British pavilion and delegation of companies to showcase the UK as a tech superpower. In June, we will host a delegation of French scale-ups and investors going to London Tech Week, where there will be a programme of activities to support companies interested in expanding to the UK. There is a lot of momentum and we are keen to seize the opportunities in this fast-changing tech sector by strengthening and building new commercial ties and partnerships between the UK and France.

Vive l'entente cordiale et vive l'amitié franco-britannique !

British Embassy in Paris

The security challenges facing a global telecom operator.

Digital transformation, one of the essential vectors for the growth of organisation, has a direct influence on increasing the attack surface and complexity of cyber issues. The huge volume of data passing through BT's infrastructures (> 1 Tera byte /s) puts us in a prime position to analyse the global internet and anticipate threats.

It's in our DNA to offer our customers the know-how we have developed in-house over many years to protect our own infrastructures. We drink our own Champagne! Faced with increasing cyber-attacks, "cloudification", risks associated with third parties, the explosion in the number of connected objects and changes in working practices, senior executives recognise that cyber-risks can damage their business, their reputations and more. As a result, it has become a key item on the agenda of boards of directors.

Nicolas Huguet

President, BT France

II

Challenges for businesses: **The cyber landscape in 2024**

Richard Absalom,
Principal Research Analyst,
Information Security Forum Limited (ISF)

The era of the polycrisis

Amid political and economic uncertainty, social fragmentation, geopolitical tensions and environmental deterioration, the world is entering the era of the polycrisis: multiple crises occur simultaneously. At the same time, technology continues to advance and innovate at pace, promising solutions to some of the crises but exacerbating others. Governments, regulators and businesses are struggling to keep up with such change. This two-pronged threat landscape is ripe for exploitation: cyber criminals, hacktivists and state-backed hacking groups are thriving.

The nature of cyber crime makes it borderless: threats can come from anywhere, are difficult to attribute, and it is almost impossible to seek justice against the perpetrators. Therefore, organisations in both France and the UK face a range of similar challenges that could prevent them from doing business. The cyber landscape in 2024 is centred around artificial intelligence (AI)-related threats, extortion through techniques such as ransomware and data theft, continued cloud adoption and supply chain risk, and escalating regulation as lawmakers attempt to get to grips with it all. To continue operating and trading, businesses need to consolidate their efforts towards the goal of achieving business resilience. Addressing this challenge goes beyond the remit of individuals or security teams. It demands cross-organisational solutions, and a culture of cooperation between businesses.

AI brings opportunity and risk

AI continues to dominate the headlines, with advances in generative AI tooling such as ChatGPT grabbing attention. Such technology promises huge advances in efficiency and innovation, and businesses are understandably keen to adopt it quickly to prevent being left behind by competitors. However, while there are plenty of benefits to AI, there are many risks that businesses need to be aware of. These include:

- **Ensuring the integrity of information used and created by AI systems** – biased or incorrect training data can lead to poor quality outputs that compromise trust, eventually rendering the system useless.
- **Compliance with ethical and legal requirements** – the use of personal data can create potential legal issues if used without consent, and biased outcomes due to bias in learning datasets can create ethical and reputational challenges.
- **The emergence of 'Shadow AI'** – business users are buying and adopting AI systems without oversight from IT or security teams, which can lead to compromise of organisational data and introduction of new vulnerabilities.
- **Enhanced cyber attacks** – malicious actors are using AI tools to enable faster, more sophisticated, larger scale attacks (e.g. by automating vulnerability identification).
- **Malicious use of deepfakes** – accurate digital imitations of real people can be used to spread fake news, with potential for serious and damaging political impacts. Outside the political sphere, they can also enable sophisticated phishing, spear phishing (i.e. phishing attacks targeting a specific individual) and whaling attacks (i.e. phishing that targets a very senior individual).

How organisations can prepare for AI-related threats:

- Corporate boards must **take a central role** in overseeing deployment of AI systems across the organisation.
- Security teams need to **align closely with business objectives**: understand the requirement for specific AI systems and inform business stakeholders of the risks.
- Security teams should **deploy AI-enhanced security controls** to keep pace with attackers.
- People at every level of the organisation should receive **education and training on the risks of AI**, and how to identify potential deepfakes and AI-based social engineering. They should be empowered to take action when they think something is wrong.

Businesses continue to be plagued by ransomware and triple extortion

Cyber criminals follow the money, and extortion techniques such as ransomware are a lucrative, low-risk, high-reward market for them. Ransomware is big business and is run as such; a full underground industry is complete with product developers, brokers and 'as a service' offers for those criminals who do not have technical skills but want a piece of the action.

Ransomware continues to be one of the most common threats faced by organisations both in the UK and France – and they are also some of the most-targeted nations in the world. Between April 2022 to March 2023, 163 UK organisations suffered attacks (second only to US organisations), while France was the fifth most-targeted country with 108 known attacks.

However, fewer organisations are now paying ransoms – only 29% of victims did so in the final quarter of 2023 – so criminal groups are changing their tactics. Organisations now face triple extortion threats, whereby the attacker not only encrypts and denies access to systems and information, but also exfiltrates data and threatens to leak it, and then intimidates the victim organisation's customers, employees or other stakeholders. Businesses on both sides of the channel must remain vigilant and resilient against this evolving threat.

How organisations can prepare for, respond to and resume business after a ransomware attack:

- **Prepare** by focusing on cyber hygiene and system resilience (including making regular system backups); rehearsing attacks; and maintaining response plans.
- **Respond** by effectively communicating and collaborating with employees, suppliers and customers; managing staff through traumatic events; reviewing organisational governance; and assessing safe and pragmatic technological options to resume operations.
- **Resume** by supporting systems restore; resuming good governance and compliance; preparing to stop or respond to the next attack by resetting behaviours and applying lessons learned.

[1] *"Ransomware in France, April 2022–March 2023", Malwarebytes, https://www.malwarebytes.com/blog/threat-intelligence/2023/04/ransomware-review-france*

Click here

[2] *"New Ransomware Reporting Requirements Kick in as Victims Increasingly Avoid Paying", Coveware, https://www.coveware.com/blog/2024/1/25/new-ransomware-reporting-requirements-kick-in-as-victims-increasingly-avoid-paying*

Click here

Cloud adoption opens the door to supply chain attacks

Adoption of cloud services continues to increase, with all the related business benefits around scalability and elasticity. However, there are risks. Relying too much on one cloud provider can end up with 'vendor lock-in', where businesses are unable to escape from a relationship that is becoming ever more expensive. And as the common saying goes among security professionals: "Using the cloud is just using someone else's computer." Cloud service providers are key suppliers and provide an inviting attack vector for bad actors: compromising one cloud provider may open the gates to many of their customers, as seen with various incidents such as state-backed hackers compromising Microsoft and gaining access to multiple customers' Outlook accounts.

While they do invest a lot in security, the three major cloud providers – Google, Microsoft and Amazon – power 66% of global cloud infrastructure, and as such make for challenging but highly rewarding targets. Sophisticated attackers, including nation state-backed groups, know they could do a lot of economic damage if they managed to take down one of these vendors, if only for a matter of hours. Even accidental outages on the part of these providers have been shown to have significant consequences to industry.

In addition, challenges over data sovereignty remain. French companies must ensure that data is stored and processed within EU countries, or those with an equivalency agreement. UK GDPR currently has equivalency with EU GDPR, but deviates in some areas and any future changes may make cross-channel data transfer and trade more difficult.

How organisations can use cloud services securely:

- **Assess and assure** the security of cloud service providers.
- **Identify** business-critical services and build redundancy (e.g. by having the ability to revert to on-premise systems, or having backup cloud providers ready to step in if the primary one goes down).
- **Monitor** for changes in data regulations and be prepared to adjust accordingly.

[3] *A. Scroxton, "Microsoft finds Storm-0558 exploited crash dump to steal signing key", Computer Weekly, 7 September 2023, https://www.computerweekly.com/news/366551272/Microsoft-finds-Storm-0558-exploited-crash-dump-to-steal-signing-key*

Click here

[4] *F. Richter, "Amazon Maintains Cloud Lead as Microsoft Edges Closer", Statista, 5 February 2024, https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/*

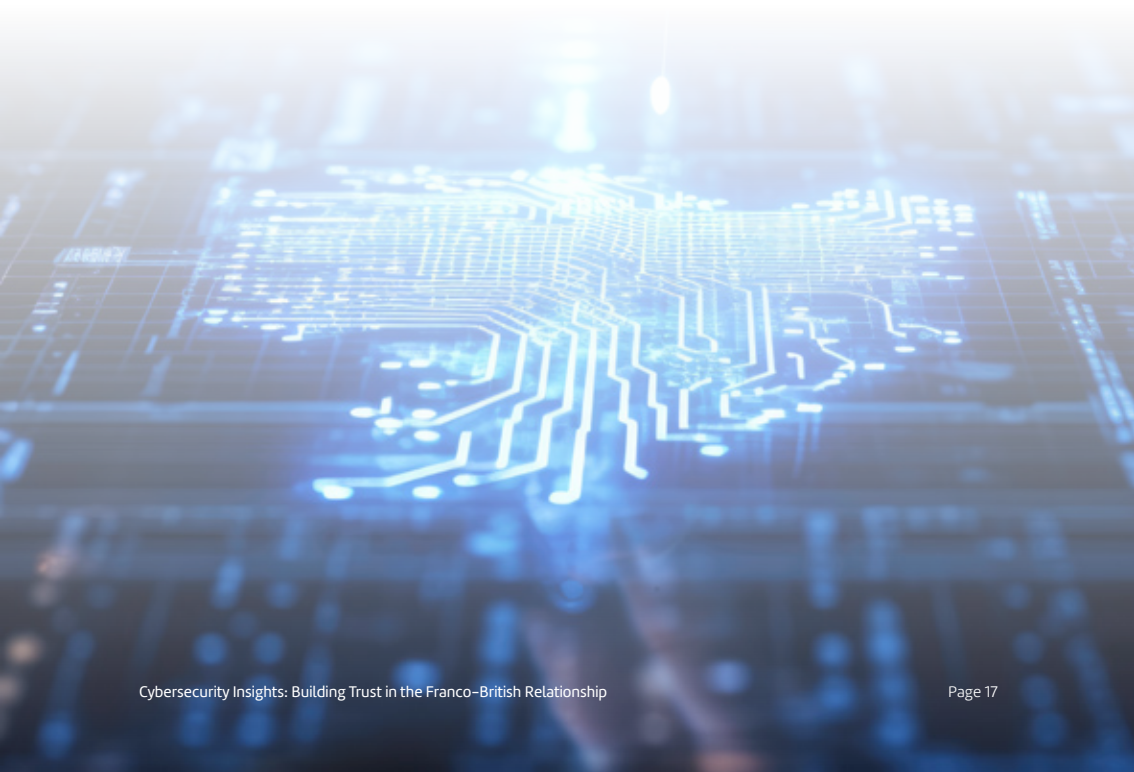
Click here

Regulatory obligations escalate

Over the next 12 months, several regulations will either be introduced, updated, or reviewed. EU GDPR may receive stringent reinforcements in 2024; NIS2 will become active in October 2024, DORA will apply to financial entities across the EU in January 2025; the EU AI Act was approved in March 2024. Non-compliance could lead to severe legal, financial, and reputational consequences. Senior individuals will have to take responsibility for ensuring their organisation complies with all relevant regulations, meaning that there will be personal accountability and consequences as well.

How organisations can be ready for incoming regulation:

- **Develop** a comprehensive understanding of the regulations in the jurisdictions where the business operates.
- **Build** necessary processes and frameworks proactively; once these regulations are enforced, adjusting to them retrospectively will be challenging.
- **Architect** the IT environment to be able to adhere to different regulations across geographical regions.



Conclusion: Resilience is key

The scale of the polycrisis and the cyber threats that it is driving in 2024 mean that it really is a matter of when, not if, an organisation suffers a cyber-attack. The summer's Olympic Games in Paris mean that France in particular has a target on its back: various groups may wish to disrupt such a prestigious event. With that in mind, organisations should focus on becoming business resilient. This means not only doing their utmost to prevent cyber attacks, but preparing to respond and recover while maintaining operations when the inevitable happens.

To build resilience, there are three core actions for businesses to consider:

Identify the organisational crown jewels, i.e. mission-critical assets, to plan and improve protections around them.

Evaluate supply chains to prepare for interruption and emergencies.

Support the workforce to deal with greater volumes of incidents, disruptions and changes.

Businesses on both sides of the channel are in this together: all face similar threats. They can cooperate by sharing information, spotting threats, containing them, and learning lessons from each other's experience. Such collaboration will help to build resilience, maintain operations and enhance trade.

The cyber challenges facing an international logistician.

Groupe Sterne operates premium low-carbon logistics services in France and internationally on a B2B basis.

The Group experienced strong organic growth between 2017 and 2022, and in parallel has carried out several major external growth operations since 2018.

This very quickly contributed to making the IT landscape more complex and heterogeneous.

The IT Department had to define a master plan combining the rationalisation and modernisation of information systems, while embarking on a vast digital transformation leading to the multiplication of information flows with the Group's customers and partners.

In this context, it was essential to include a strict cyber approach to enable controlled integration of the various entities and a drastic reduction in technical debt.

Groupe Sterne therefore committed itself very early on to implementing standards linked to information security (ISO 27001) and personal data protection (ISO 27701) to structure its approach and offer its customers the highest level of confidentiality and security.

Boris Pouderous

CIO, Sterne group

Cybersecurity at Eurostar is managed in a unified way whether people, systems and datacenters are in the UK or Continental Europe. Besides our ISO 27001 certification, our cybersecurity operations are based on the NIST (National Institute of Standards and Technology) Cybersecurity framework. **Our approach covers People, Process and Technology.** Regular controls are in place to detect vulnerability and non-conformities, resulting in additional measures to safeguard the security of our systems. Identification of our assets and threat management are essential to adapt our priorities and fine tune our detection and protection capabilities. All Eurostar staff members receive appropriate and regular information and training on security awareness. Differences in domestic regulations might force us to have specific approaches in the UK and Continental Europe. This would reduce our overall efficiency and might hinder our corporate cybersecurity approach.

Olivier Leprêtre

Cybersecurity Director, Eurostar

III

Regulatory framework and compliance

France Charruyer,
Founder, Lawyer & Partner, IP, IT & Data, Altij

Nicholas Cullen,
Lawyer, Partner, Data, IT & Corporate,
Solicitor of England and Wales, Altij

> *Now, here, you see, it takes all the running you can do, to keep in the same place. If you want to get somewhere else, you must run at least twice as fast as that!*
>
> *Lewis Carroll, Through the Looking Glass*

Introduction and overview: regulatory responses to a shared challenge

The role of cybersecurity legislation in the "Digital Decade"[1]

In a cybersecurity context characterised by instability and unpredictability, the challenge for legislators is to provide clear and legible laws and standards which are adequate in the face of multiple and evolving threats. To be effective, these laws have to give compliant organisations an advantage in protecting their critical assets.

Over the coming decade, the countries and geopolitical blocs which are best able to defend their institutions and economies from cyber-threats will obtain significant strategic advantages.

[1] *The phrase comes from a European Commission policy programme: "Europe's Digital Decade: digital targets for 2030"*

In response to this common challenge, legislators on both sides of the Channel continue to reinforce their regulatory frameworks. Both France and the UK consider cybersecurity as essential to their vital interests, with both adopting national strategies in this area:

Table 1: Strategic cybersecurity planning in France and the UK

	FRANCE	UK
Defence	**2024–2025 Military Planning Law** €4 billion of cybersecurity requirements over the period 2024-2030. Aims to "continue to develop first-rate cyber defence, robust and credible in the face of strategic competitors, capable of ensuring the resilience of the Ministry's critical activities and interoperability with allies over the long term." The law also impacts software publishers, who have an obligation to notify significant vulnerabilities affecting their products to the French cybersecurity agency (ANSSI).	**Cyber Resilience Strategy for Defence 2022–2030** Central aim: • Defence's critical functions to be "significantly hardened to cyber-attack" by 2026, • all Defence organisations "resilient to known vulnerabilities and attack methods" no later than 2030.
Public sector	**"Cloud at the centre" doctrine** Aims to implement the use by the state of cloud computing solutions that are more secure and "immune" to non-EU law, in particular by implementing a standard called "SecNumCloud" An equivalent European standard called the EUCS is currently being prepared by the EU cybersecurity agency, ENISA – with negotiations ongoing on possible data localisation and sovereignty requirements.	**Government Cybersecurity Strategy** Strategy based on two "pillars": (1) foundation of organisational cybersecurity resilience and (2) 'defend as one': sharing cybersecurity data, expertise and capabilities across organisations, with a focus on five objectives: (1) managing cyber-risk, (2) protecting against cyberattack, (3) detecting cybersecurity events, (4) minimising the impact of incidents and (5) developing the right skills knowledge and culture.

Key points in common: board-level accountability and liability, management of supply chains, training of staff

In many respects, the changes and updates to cybersecurity laws in France and the UK show a common direction of travel. Both the EU and the UK have either taken steps to reinforce and extend their respective Network and Information Security legislations or are planning to do s[2]o. This ongoing regulatory evolution requires organisations in both France and the UK to improve their cybersecurity governance, including, in particular:

Increased **accountability for management bodies**, which must now **take direct responsibility for cybersecurity.**

Implementation of so-called **"by design" obligations** (building in privacy and security in information systems).

Reinforced **technical and organisational cybersecurity requirements.**

Stricter **alert and notification requirements**[3] for incidents and breaches (including horizontal reporting, encouraged through legal protections of whistleblowers).

Duties to **check the data security levels of suppliers** and to require **appropriate contractual guarantees** from them (protecting the value chain).

Responsibility for ensuring staff **receive appropriate cybersecurity training.**

[2] *Thus, the "NIS 2" Directive will come into force in France by October 2024 at the latest, while in the UK, the Government carried out a consultation exercise in 2022 and has since announced its intention to update the UK NIS Regulations as soon as parliamentary time allows.*

[3] *For example, in France, a 2023 Interior Ministry programming law creates an obligation for organisations to make a criminal complaint within 72 hours of becoming aware of a cyberattack, in order to benefit from insurance coverage (Loi d'orientation et de programmation du ministère de l'intérieur du 24 janvier 2023 – Article 5).*

Ongoing cross-border cooperation at EU and bilateral level

Government and law enforcement in France and the UK continue to work together to combat cybersecurity threats. Thus, in December 2023, the EU and the UK held their inaugural Cyber Dialogue in Brussels[4] under the EU-UK Trade and Cooperation agreement, which establishes principles on cyber issues, including dialogue on policy developments, sharing of best practices, and cooperation between bodies such as cybersecurity agencies and emergency response teams[5].

Acting bilaterally, France and the UK organised a conference at Lancaster House in London on 6 and 7 February 2024, with discussions centring on concerns around the proliferation and irresponsible use of cyber-intrusion capabilities available on the market[6].

Cooperation continues between law-enforcement agencies. Thus, in February 2024, the UK's National Crime Agency (NCA) announced that an international coalition of agencies in 10 countries, including France and the USA, had taken control of the infrastructure of hacking group Lockbit[7].

At the EU level, the proposed "Cyber Solidarity Act", on which political agreement was reached in March 2024, establishes a European "Cybersecurity Alert System", made up of a network of "Cyber Hubs" across the EU, as well as a "Cybersecurity Emergency Mechanism" which aims to enhance preparation and response to significant and large-scale cyber-incidents.

[4] https://www.eeas.europa.eu/eeas/cyber-eu-and-uk-launch-cyber-dialogue_en

[5] EU-UK Trade and Cooperation agreement: Part Four: Thematic cooperation, Title II: Cybersecurity

Click here

[6] https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-numerique/actualites-et-evenements/article/cybersecurite-communique-conjoint-de-la-france-et-du-royaume-uni-sur-la#:~:text=Les%206%20et%207%20février,cyber%20disponibles%20sur%20le%20marché.

Click here

[7] See https://www.reuters.com/technology/cybersecurity/us-indicts-two-russian-nationals-lockbit-cybercrime-gang-bust-2024-02-20/

Click here

A holistic approach to compliance: transparency and trust

Organisations active in both the UK and France should be aware that, while there are legal and cultural differences between the two countries, the overall legislative landscape demands a holistic and joined-up approach to cybersecurity.

Key concepts include accountability, risk management and governance, in a context where cybersecurity compliance is increasingly becoming a performance indicator for businesses, with investors including cybersecurity in their due diligence processes.

Common regulatory baseline: GDPR and NIS

Compliance and legal teams in France and the UK will find many points of similarity between the two countries' respective legal landscapes.

In particular, the General Data Protection Regulation (GDPR), in its UK and EU versions, provides a framework for the security of personal data, now firmly established in corporate cultures in France and the UK, in addition to sector-based obligations for certain actors[8].

Both jurisdictions also impose "Network and Information security" (NIS) requirements on operators of essential services and some providers of digital services. Like GDPR, the NIS requirements have a common source in EU law[9]. They have also been subject on both sides of the Channel to legislative updates, particularly with the EU's NIS2 directive, due to come into force in France by October 2024.

As summarised in the table below, the obligations in each jurisdiction are essentially comparable and, in some respects, identical in respect of personal data.

[8] In addition to the GDPR and NIS frameworks, there are sources of cybersecurity obligations for companies in the UK and France, applicable to specific actors and sectors. Without aiming to list these exhaustively, examples include, in France, specific requirements for actors in the healthcare sector to use hosting service providers with an "HDS" certification similar to ISO27001 and in the UK, enhanced cybersecurity requirements for providers of public telecommunications networks and services under the Communications Act 2003, as amended by the Telecommunications (Security) Act 2021. In addition, in both the UK and France, there are specific requirements for "Trust" service providers which verify the identity of individuals online, under eIDAS (electronic identification and trust services) regulations, to notify the competent authorities of a security breach within 24 hours.

[9] Network Information Security (NIS) Directive - 2016/1148)

Table 2: GDPR and NIS

	FRANCE	UK
GDPR (personal data processing)	**EU GDPR** Additional rules contained in the 1978 Computing and Liberties law, as updated. Enforcement by the *Commission Nationale de l'Informatique et des Libertés* (CNIL). Article 5.1(f): Ensure appropriate security when processing personal data.	**UK GDPR** Additional rules contained in the Data Protection Act, 2018 Enforcement by the Information Commissioner's Office (ICO) Article 5: Ensure appropriate security when processing personal data.

GDPR
(personal data processing)

FRANCE	UK
Article 28: Mandatory guarantees from data processors. Article 32 General security obligation: - Implement appropriate technical and organisational measures to guarantee a level of security appropriate to the risk, - Possible measures include pseudonymisation, encryption, guaranteeing system integrity, data recovery mechanisms in the event of an incident, regular testing procedures, etc. Articles 33 and 34: Requirements to notify CNIL of personal data breach and to inform affected data subjects. Article 83: - CNIL can impose administrative finds of up to €20 million or 4% of total worldwide annual turnover, whichever is higher (for breaches relating to basic principles of processing or data subjects' rights). - For a breach of article 32, CNIL can impose administrative finds of up to €10 million or 2% of total worldwide annual turnover, whichever is higher	Article 28: Mandatory guarantees from data processors. Article 32: General security obligation: - Implement appropriate technical and organisational measures to guarantee a level of security appropriate to the risk, - Possible measures include pseudonymisation, encryption, guaranteeing system integrity, data recovery mechanisms in the event of an incident, regular testing procedures, etc. Articles 33 and 34: Requirements to notify ICO of personal data breach and to inform affected data subjects. Article 83: - ICO can impose administrative finds of up to £17.5 million or 4% of total worldwide annual turnover, whichever is higher (for breaches relating to basic principles of processing or data subjects' rights). - For a breach of article 32, ICO can impose administrative finds of up to £8.7 million or 2% of total worldwide annual turnover, whichever is higher

NIS
Network and Information Security

FRANCE	UK
French transposition Law no. 2018-133 containing EU law security provision. (N.B. Due be updated by October 2024 at the latest by the NIS2 Directive) Applies to: 1. *Opérateurs de services essentiels* (OSE): energy, transport, banks, financial markets, health, water, digital infrastructure. 2. *Fournisseurs de services numériques* (FSN): online marketplaces, search engines, cloud computing services. Regulated by the national cybersecurity agency (*Agence nationale de la sécurité des systèmes d'information* – ANSSI) Obligations include: ✓ Identification of OSEs and their essential information systems to ANSSI, ✓ Application of specific security requirements, ✓ Reporting of incidents to ANSSI Articles 9 and 15: Fines of between €75,000 and €125,000 for directors in breach of various provisions of the law. **N.B.** The NIS2 Directive will significantly reinforce powers to fine companies for non-compliance – *see Table 4 page 29.*	**The Network and Information Regulations 2018 (NISR)** (N.B. Updated in 2020. Further update to be carried out, dependant on Parliamentary calendar) Applies to: 1. Operators of essential services (OESs): energy, transport, health, water, digital infrastructure 2. Relevant digital service providers (RDSPs): online marketplaces, search engines, cloud computing services. Regulated by ICO for RDSPs and by the relevant Government department for OESs. Obligations include: ✓ Identification of OESs to their competent authority, ✓ Application of specific security requirements, ✓ Reporting of incidents to competent authority Section 18: Penalties can be imposed by the ICO or the competent authority if different of up to £17 million for a material contravention which has or could cause *"an incident resulting in an immediate threat to life or significant adverse impact on the United Kingdom economy"*

NB. Regulatory guidelines and "Soft law"

In addition to the "hard" legal obligations discussed in this section, public institutions and regulatory authorities (e.g. ANSSI, CNIL and cybermalveillance.gouv.fr in France, and in the UK the NCSC and the ICO) publish guidance on cybersecurity best practice. There are also associations and professional bodies on both sides of channel (e.g. CLUSIF, CESIN, CIGREF in France, CIISec and the UK Cyber Security Council in the UK) which work to support business and cybersecurity professionals in this area.

On a European Level, ENISA (the European Agency for Cybsersecurity) is currently preparing its "State-of-the-Art" documents for the EU's EUCC Certification scheme (European Cybersecurity Certification Scheme on Common Criteria", based on an implementing regulation published by the European Commission in January 2024.

Given that article 32 of GDPR requires controllers and processors to take into account "the state of the art", companies should be aware of these regulatory best practice guidelines and adapt their processes accordingly.

Table 3: Examples of regulatory guidelines

	FRANCE	UK
Cybersecurity	**Agence Nationale de la sécurité des systèmes d'information (ANSSI)** Provides a series of resources for business on its website, including good practice guidance aimed at management and IT security professionals.	**National Cyber Security Centre (NCSC)** Publishes guidance including the "Cyber Security Toolkit for Boards", with aims including embedding cybersecurity into your organisation.
Personnal Data	**Commission Nationale de l'Informatique et des Libertés (CNIL)** Regularly publishes practical and technical guidance and news on cybersecurity, including its updated practical guide to personal data security published in March 2024.	**The Information Commissioner's Office (ICO)** Publishes security guidance for respectively, large organisations in the public, private and third sectors, as well as small businesses through its small business web hub.

Ongoing reforms in the EU, France and the UK

Legislators in France, the UK and the EU continue to adapt and update cybersecurity requirements, to confront the increasingly severe threat level.

Allowing for legal and cultural differences, there are various principles on which both jurisdictions are aligned in their approach to cybersecurity, including:

- A strengthening of the general obligation to ensure cybersecurity, which public and private sector organisations will have to integrate into their practices in security planning and technical and organisational resilience, as well as the state of the art,
- Accountability explicitly focused on the highest levels of the organisation, under the EU's NIS2 and DORA legislation, but also under the UK's proposed GDPR reform, in which a "Senior Responsible Individual" will have responsibility for monitoring data security and training[10].
- To ensure that cybersecurity training because the rule and not the exception
- To enable international cooperation and coordination on cybersecurity[11].

[10] Directors of UK companies also have defined duties under articles 170 to 177 of the Companies Act 2006, including to promote the success of the company and to exercise reasonable care, skill and diligence. The former provision is cited by the UK NCSC' "Cyber Security Toolkit for Boards".

[11] The NIS2 directive contains an extended section on cooperation at Union and International Level, including the creation of an EU Cooperation Group, a network of national "CSIRTs" (computer security incident response teams) the establishment of the European cyber crisis liaison organisation network (EU-CyCLONe) and the possibility to conclude international agreements with third countries to allow their participation in the activites of these three groups.

Table 4: Examples of key legislative updates in cybersecurity

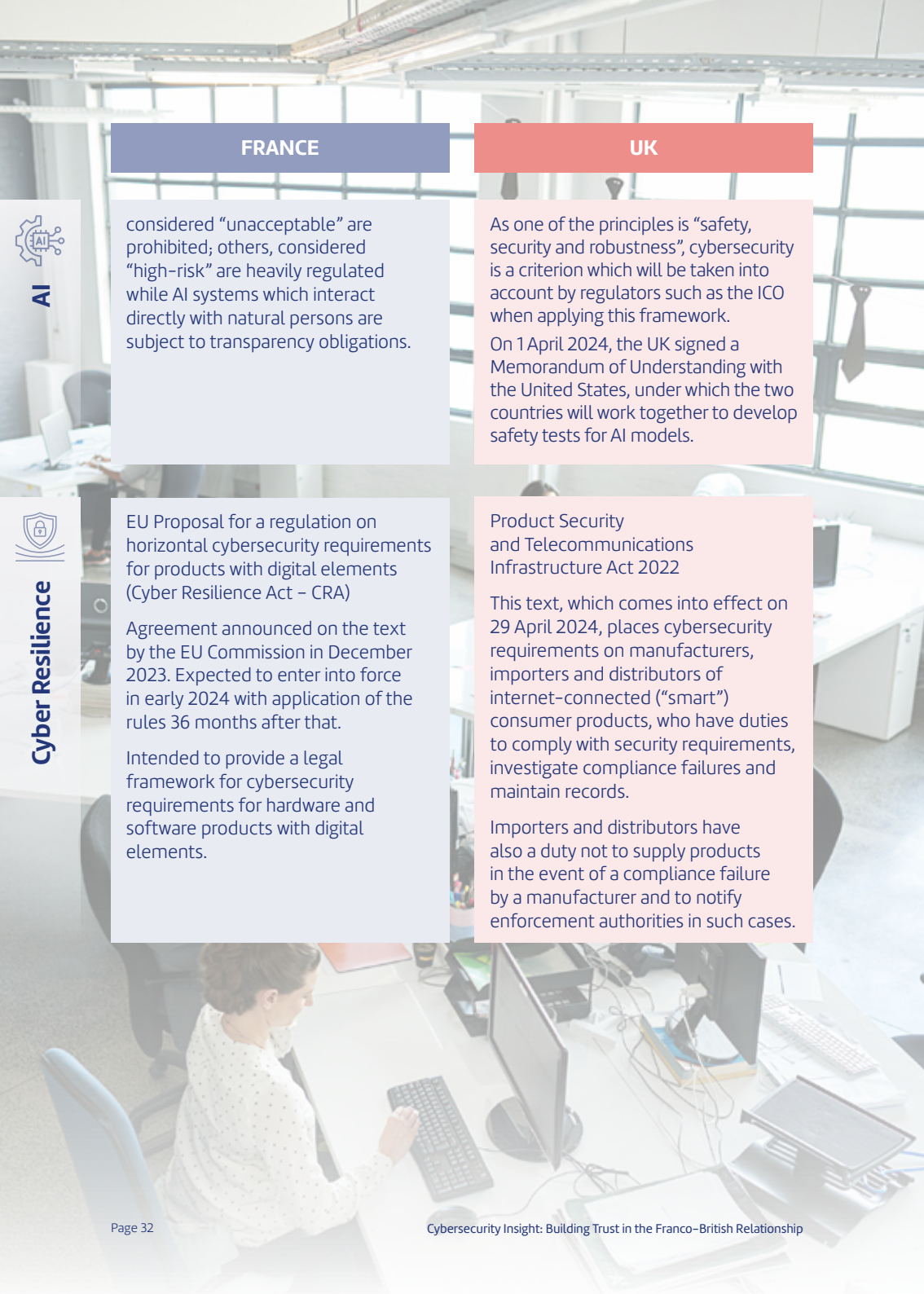
FRANCE	UK
EU GDPR remains in force *(see Table 2 page 25-27)*	**Proposal to reform UK GDPR currently before Parliament.** Data security provisions not directly amended by the proposed reform. However, Data protection officer (DPO) will be replaced by a "Senior Responsible Individual" who must be part of the organisation's senior management, and who will have responsibility for, among other things, monitoring compliance with Article 32 of UK GDPR.

Personal data

Network and Information security

FRANCE	UK
EU "NIS 2" Directive 2022/2555: transposition into French law before 18 October 2024 Increases the scope of the sectors concerned to include "essential and important entities" (e.g. public administrations, telecommunications, social networking platforms, postal services, space sector, etc.) and introduces stringent requirements in terms of risk management, incident reporting and security measures. ANSSI will provide clarification on the scope of the regulated entities and the security measures to put in place. Article 20 places increased responsibility for cybersecurity on management bodies to approve risk-management measures and oversee their implementation, as well as training obligations in cybersecurity. Such bodies can be held liable for infringements of cybersecurity requirements. Article 34: Possible fines for breaches Essential entities: Administrative fines of a maximum of at least €10 million or 2% of total worldwide annual turnover (whichever is higher) Important entities: Administrative fines of a maximum of at least €7 million or 1,4% of total worldwide annual turnover (whichever is higher)	Currently in place: The Network and Information Systems Regulations 2018, as updated in 2020 *(See Table 2 page 25-27 for scope)* **N.B.** Proposal to update the NISR: Following consultation, Government has announced intention to move ahead with reform. Expands definition of relevant digital service providers (RDSPs) to include "Managed Service Providers" (MSPs), meaning companies which manage elements of their customers' IT systems remotely. Because these actors have access to the systems of a large number of customers, they potentially represent a systemic risk in the event of a cyber-attack. Also aims to introduce a "two-tier" supervisory regime for digital service providers: a new "proactive supervision" tier for the most critical providers, alongside the existing "reactive" supervision tier for all other concerned entities. *(See Table 2 page 25-27 for penalties in force)*

	FRANCE	UK
Financial services	DORA *(Digital Operational Resilience Act)* Regulation (EU) 2022/2554 Comes into force on 17 January 2025. Aims to improve the digital operational resilience of financial services providers in risk management of information and communication technologies (ICT), notification of incidents and cyber threats to the authorities; digital operational resilience tests; sharing of information and intelligence relating to cyber threats; and risk management measures linked to third-party ICT service providers. As with NIS2, **a key aspect is the direct responsibility of management bodies.**	Regulation through the Financial Conduct Authority (FCA) and through the Bank of England's Prudential Regulation Authority (PRA), which have statutory duties to combat financial crime and protect the UK financial system. The FCA's Handbook contains Principles including Principle 3 which requires a firm "**to take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems**". The FCA has significant enforcement powers and in October 2023 imposed a fine of £11million following a major data breach affecting the customers of a credit rating agency.
Artificial intelligence / AI	EU "AI Act" (Regulation laying down harmonised rules on Artificial Intelligence), agreed between Council and Parliament in December 2023, endorsed by Member States in February 2024 and endorsed by the European Parliament in March 2024. Final text contains specific cybersecurity requirements for high-risk AI systems, including "by design" and resilience obligations. The AI Act takes a graduated, risk-based approach: certain systems,	Government White Paper "A pro-innovation approach to AI regulation" published in March 2023. "Agile" approach under which *"We will not put these principles on a statutory footing initially. New rigid and onerous legislative requirements on businesses could hold back AI innovation and reduce our ability to respond quickly and in a proportionate way to future technological advances. Instead, the principles will be issued on a non-statutory basis and implemented by existing regulators."*



	FRANCE	UK
AI	considered “unacceptable” are prohibited; others, considered “high-risk” are heavily regulated while AI systems which interact directly with natural persons are subject to transparency obligations.	As one of the principles is “safety, security and robustness”, cybersecurity is a criterion which will be taken into account by regulators such as the ICO when applying this framework. On 1 April 2024, the UK signed a Memorandum of Understanding with the United States, under which the two countries will work together to develop safety tests for AI models.
Cyber Resilience	EU Proposal for a regulation on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act – CRA) Agreement announced on the text by the EU Commission in December 2023. Expected to enter into force in early 2024 with application of the rules 36 months after that. Intended to provide a legal framework for cybersecurity requirements for hardware and software products with digital elements.	Product Security and Telecommunications Infrastructure Act 2022 This text, which comes into effect on 29 April 2024, places cybersecurity requirements on manufacturers, importers and distributors of internet-connected (“smart”) consumer products, who have duties to comply with security requirements, investigate compliance failures and maintain records. Importers and distributors have also a duty not to supply products in the event of a compliance failure by a manufacturer and to notify enforcement authorities in such cases.

Conclusion: The Red Queen's paradox

Cybersecurity legislation aims to provide a stable framework under which the rule of law can apply to the online space.

Key objectives are to encourage and promote risk management, improved governance structures and the development of necessary skills within organisations: all of which require engagement and leadership from boards. Businesses thus need to build expertise and achieve organisational resilience within a culture of accountability and shared confidence.

This extends to the evaluation and general reinforcement of actors all along supply chains, including the SMEs which form the bedrock of the economy in both the UK and France – corresponding to the "whole-of-society" approach to cybersecurity encouraged in the UK's National Cyber Strategy. While operational disruption and loss of data can have varying impacts depending on an organisation's size and activities, increased interdependence of IT systems means that the cybersecurity of third parties is a major issue for most businesses.

Thus, the implementation of standards, best practices and certifications to be at the state of the art requires a continuing effort all along the supply-chain, involving employees, external partners, suppliers and customers.

Faced with these challenges, management needs to provide the lead in terms of raising awareness, allocating budgets and managing risk within their organisations.

A further issue is reinforcing and scaling up systems of threat detection and defence in a context where AI systems are potentially available to bad actors and to information security teams alike. Organisations thus need to make appropriate investments and develop new skills and expertise to interact with these systems, recalling the terms of the Red Queen's paradox: "it takes all the running you can do, to keep in the same place".

The emergence of AI is also reshaping geopolitical dynamics, with hybrid AIs for civilian and military use available on a global scale. In this context, nation states and geopolitical blocs are also engaged in a race for talent and funding to extract economic value and control the risks involved.

Cybersecurity law cannot therefore be purely reactive: it has to anticipate future risk and provide a framework which is both robust and flexible enough to be adapted to new technological challenges.

Laws are in many ways more fragile than the technologies they regulate and both the EU and UK approaches converge on the need to go beyond a pure "security by design" approach and find the right risk/reward ratio: assessing an acceptable level of risk, retaining control over digital assets and protecting our societies.

The challenge now is to ensure that the next generation of cybersecurity regulation can be implemented in practice, with a shared goal of protecting our vital assets, our way of life and our democratic values against increasing cyber-threats, in the interest of our common future.

Getlink, delivers high quality and secure mobility services across Europe. **Digitalisation being a cornerstone of our strategy, Cybersecurity is a priority and is embedded.**

This challenge is global and, as a bi-national company, we must consider both sides of the Channel. Cybersecurity is managed at all levels, starting from the bi-national main Board who implement policy, and check strategies and dashboards quarterly, down to operational IT teams on both sides. We are subject to both British and French regulations - differently shaped but with similar content. Our policies, organisation and tools deliver a security level that is aligned with these rules. We report regularly to the authorities: ANSSI (Agence Nationale de la Securité des systems d'information - France), DFT (Department for Transport – UK), Ofgem (Office of Gas and Electricity Markets – UK). We invest significant resources in efficient technologies, including on AI, and on highly skilled staff

John Keefe

Chief Corporate and Public Affairs Officer, Getlink Group

IV

Cybersecurity Governance

The key to cyber resilience

David Mudd
Global Head of Digital Trust Assurance,
British Standard Institution (BSI)

bsi Your partner in progress

What is cybersecurity governance?

Cybersecurity governance is the process for controlling and directing an organisation's cybersecurity activities. It calls for a holistic approach to cybersecurity that integrates with organisational operations to prevent business interruptions due to cyber threats or attacks. Key features of cybersecurity governance include:

- Accountability framework
- Decision-making hierarchies
- Defined risks related to business objectives
- Risk mitigation strategies and plans
- Oversight processes and procedures

Why is cybersecurity governance important?

The vast majority of organisations in the UK and France are heavily dependent on digital technologies to operate their businesses. The huge expansion of the digital economy has also expanded the level of cybersecurity threats. The resultant increasing and evolving regulatory landscape is causing further business risks, with significant fines for non-compliance. The potential impact of cyber incidents is severe: "cyber-risk is no longer just an IT problem; it is a critical vulnerability that directly influences the health of the collective enterprise." [David Raissipour, Forbes 2023].

In today's increasingly digital economy, cybersecurity risk needs a similar focus as financial and legal risk due to its potential material impact on business. There is an intrinsic link with business resilience that requires directors and boards of all organisations to engage with cybersecurity to gain an understanding of their exposure to cybersecurity risk, evaluating how it aligns with their risk appetite and business strategy. Good cybersecurity governance will enable them to capitalise on the opportunities that the digital economy presents, whilst effectively managing the associated risks.

Furthermore, at the macro level, for society as a whole to benefit from digital technologies to deliver new and improved experiences and quality of life that is sustainable, organisations need to take a robust position on cybersecurity governance to minimise the impact of cybercrime, which is effectively the 3rd largest economy in the world and growing.

With regard to the impact of cybersecurity governance on business, every business has some kind of cybersecurity posture. An organisation could spend its entire resources on cybersecurity and there would still be residual risk. Conversely an organisation could invest nothing at all. Somewhere between these two extremes, and organisation will decide, at a senior level in terms of cash and resource:

"this is what we are going to invest"

At this point, how comfortable are you that you truly understand what residual risk you hold and how well that aligns with your risk appetite and your business strategy?

If it aligns on one day, in the fast-paced, increasingly digital world, where your business operating model and the associated risks are changing, how well do you sleep at night knowing it aligns each day thereafter?

This is where effective cybersecurity governance helps you.

What does good cybersecurity governance look like?

Effective risk management.

Investment in risk management allows trusted risk-based decision making. This will allow businesses to engage with disruptive and differentiating digital solutions, with cybersecurity good practice supporting business decisions, rather than just dealing with the consequences.

Effective decision delegation.

Ensuring that decision makers at all levels within the business are empowered with the appropriate cybersecurity knowledge, skills and competence enables the senior management to maintain ultimate accountability for cybersecurity risk management, whilst allowing timely and effective decisions to be made to drive businesses forward.

Management of uncertainty.

The digitally-based systems businesses use today intrinsically link technology, business process and people. This complexity brings uncertainty to risk management which is to some extent unavoidable. Therefore, understanding the limitations of security controls and approaches, alongside strategies for dealing with residual and uncertain risk are key.

Effective cybersecurity risk management communication.

Effective communication is essential for directing and controlling cybersecurity risk management. Trust is built on good communication, enabling a positive cybersecurity culture (see below).

- Top-down communication needs to clearly show business direction, objectives and approach to risk, along with clear roles and responsibilities.
- Bottom-up and lateral communication needs to clearly provide detailed technical and non-technical information to inform risk management decision making.

Effective cybersecurity culture.

An effective cybersecurity culture will help deal with the complexities and uncertainties mentioned above. People are key to effective defence against a cybersecurity incident and the biggest factor in responding to, and recovering from an incident. Therefore, cybersecurity culture is an important factor in business resilience. Whilst there are many elements to creating an effective culture, the aspects above, alongside baking in cybersecurity management into a continuous "business as usual" activity will be a big step in the right direction.

Current business approaches to cybersecurity governance

Historically, cybersecurity has been seen by businesses as a technological issue which lies with the IT team. With the rapid increase in digitalization and cyber-risk, and the emergence of CISO and DPO roles, this has moved forward. However, effective cybersecurity governance is still immature.

Data from a UK Government survey in 2023 found that, though cybersecurity was seen as a high priority by senior business leaders, this had not generally resulted into clear action or ownership at board level. Some specific findings were:

30%

of businesses had board members or trustees explicitly responsible for cybersecurity

37%

of businesses reported being insured against cybersecurity risk

16%

of corporate annual reports covered cyber-risks

49%

of medium businesses and 68% of large businesses had a formal cybersecurity strategy in place

29%

of businesses had undertaken a cybersecurity risk assessment in previous 12 months

13%

of businesses reviewed the cybersecurity risks posed by their immediate suppliers

Government strategies around cybersecurity governance

UK and France have broadly similar regulatory frameworks in place as described in the previous section. Whilst there is no explicit requirement for formal governance, GDPR has been very clear on accountability and governance exemplified by the Data Protection Officer role requirement, whilst NIS2 puts a greater focus on senior management oversight of the risk management process and senior management accountability in the event of an incident. This clearly raises the profile of cybersecurity governance within the UK and French organisations.

UK Government has specifically acknowledged the importance of cybersecurity governance and the lack of maturity in this area across businesses.

- The UK National Cyber Security Centre published a suite of guidance for businesses through 2018 and 2019, resulting in the "Cybersecurity Toolkit for Boards" mentioned in the previous section.
- Last year, as a result of the survey above, the UK Government initiated a Code of Practice for Cyber Governance – issued for public comment in January 2024. The aim of this code of practice is to give clear guidance on the actions and responsibilities of board members themselves in creating effective governance, written in general business language, minimising technical jargon.

Standards and best practice for cybersecurity governance

ISO/IEC 27001 provides an excellent framework for cybersecurity governance, as it sets out requirements for policies, processes, roles, responsibilities, communication, risk assessment and management, monitoring and continual improvement. It is widely adopted across UK, with over 6,000 certifications against the standard covering nearly 12,000 sites as of end of 2022. The number is increasing significantly since the launch of the updated standard last year. In France, adoption is lower, but increasing, with over 900 certificates covering over 2,800 sites as of end of 2022. The main uptake is in the ICT sector, also accounting for digital services supporting other key sectors.

Being a global standard, certification to ISO/IEC 27001 also supports global trade, building international trust in an organisation's governance of cybersecurity, so businesses in the UK and Europe use it both for their own regional and internal business development, and as a benchmark when assessing or evaluating potential international suppliers and partners for their cybersecurity risk.

Another key framework on the global stage comes from the National Institute of Standards and Technology (NIST) in the USA. Known as the NIST Cybersecurity Framework it is a voluntary scheme principally for self-assessment. Uptake is difficult to quantity as there is no formal certification process, but, in the UK and France, there is limited evidence of adoption.

Global best practice for managing cybersecurity risk can be found in the international standard ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection. Information security management system requirements.

From ISO:

- "With cyber-crime on the rise and new threats constantly emerging, it can seem difficult or even impossible to manage cyber-risk. ISO/IEC 27001 helps organisation become risk-aware and proactively identify weaknesses.
- ISO/IEC 27001 promotes a holistic approach to information security... [and] is a tool for risk management, cyber-resilience and operational excellence."

What should UK and French businesses do now about cybersecurity governance?

1. Review your organisation's current status against the 5 factors of good cybersecurity governance listed page 37.
2. Consider how well you understand your residual cybersecurity risk and how well aligned it is with your organisation's risk appetite and business strategy.
3. Consider how well your information/cybersecurity management system supports your organisation govern risk in this area.

Tools to help you

UK Government proposed Cyber Resilience Code of Conduct. Annex A	UK Government NCSC Cyber tool kit for boards	ISO/IEC 27001:2022
Click here	Click here	Click here

The future of cybersecurity governance

With the digital economy so critical to the global economy, alongside the increasing and evolving cybersecurity risk, governments around the world are putting an increasing focus on cybersecurity governance. In the EU, the NIS2 Directive in particular focuses on governance principles and its expansion to cover more sectors will make this more relevant across industries. Alongside the imminent update to UK NIS, this will likely drive many more businesses to take a more robust position on cybersecurity governance in the UK and France.

Another key factor which will drive improved cybersecurity governance is investment market requirements for transparency and confirmation. The Securities and Exchange Commission (SEC) in the USA has added a filing requirement to cover cybersecurity governance and disclosure of incidents. This will have a knock-on effect through company supply chains which will impact businesses in the UK and France who provide services to US companies. Furthermore, a similar process is being investigated in the UK, which will put further pressure on publicly listed businesses in the UK to formalise their cybersecurity governance posture.

One further issue which will likely drive a stronger focus on cybersecurity governance is the rapid adoption of AI across businesses of all sizes in all sectors. AI bring many business advantages, but also distinct new and challenges around security and privacy. There are already major news stories around the security and privacy of AI. This significant escalation in risk will further highlight the importance of governance in cyber. A combination of further regulation e.g. EU AI Act, alongside general business risk management, with inevitable future news stories of significant incidents will likely drive improved governance across sectors through the supply chain.

To help organisations implement and maintain effective governance, ISO/IEC 27001, has a whole ecosystem of support, from training, and consultancy to assessment and certification, providing a pathway for all organisations to be able to implement and evidence effective cybersecurity governance. Other initiatives such as the UK Cyber Governance Code of Practice and the UK NCSC's Toolkit for Boards provide readily accessible guidance and tools to get started on the path. Therefore, all organisations in the UK and France, large or small, commercial or non-profit across all sectors, have the opportunity to demonstrate effective cybersecurity governance, protecting the interests of their customers, employees and all stakeholders, whilst providing competitive advantage, alongside supporting the digital transformation towards a smart society for all that is trusted and secure.

Conclusion

Cybersecurity governance drives an holistic approach, integrating cybersecurity with organisational operations and requires senior management to actively engage on this critical topic. With increasing business dependencies on digital systems, alongside a sharp increase in cybercrime and corresponding increase in regulation, cybersecurity is seen as a major business risk that needs to be governed in a similar fashion as other key business factors such as finance.

The basic principles of effective cybersecurity governance are well documented, alongside comprehensive global best practice in the form of an ISO standard. However, the process is still relatively immature across businesses. Regulation across the EU and UK is driving more focus on cybersecurity governance, which is helping raise the profile of this important aspect of business leadership.

All business leaders should be considering how well their organisation is currently governing cybersecurity, using the basic principles of effective cybersecurity governance as a guide and various governance tools and standards to support effective implementation. In particular they should consider how well they understand their residual cybersecurity risk and whether it aligns with the business risk appetite and strategy.

Effective cybersecurity governance helps build a resilient organisation that can reap the benefits disruptive digital technologies can bring whilst minimising risk. It also helps support compliance with increasing cybersecurity regulation. Ultimately, compliance with global best practice in the form of the ISO standard helps build digital trust with organisations around the world. Better for us all, as individuals, businesses and society.

With the rising prominence of legal considerations in cybersecurity, particularly within the EU regulatory context, **it is essential to shift perspective from viewing it solely as a constraint to recognizing it as an opportunity.** Organisations have the opportunity to harness the increased focus and transparency on cybersecurity as a driver for enhancing performance. This change in mindset not only fosters a more secure and compliant business environment but also empowers professionals and organisations to adeptly navigate complex regulatory frameworks by leveraging accurate legal insights. Given the Lefebvre-Sarrut Group's commitment to keeping professionals and organisations abreast of regulations, compliance standards, and industry best practices, there is a natural inclination to view cybersecurity as a catalyst for performance enhancement and structural development.

Candice TRAN DAI

Security Director, Lefebvre Dalloz

Most threat actors are purely financially motivated. They don't care where you are from, it's all about making money.

We base our security frameworks, policies and controls around the EU regulatory baseline but aim to apply them across all geographies wherever possible. We take local regulations into account on a case-by-case basis, but a country-specific approach makes little sense: threats can come from anywhere, so we aim to have the same baseline everywhere.

Guillaume Balix

Resilience Lead, CISO Office & Transformation, L'Oréal

V

Artificial Intelligence (AI):
Serving cybercriminals and those who fight them

Nicolas Arpagian
Vice-President, HeadMind Partners
Senior Lecturer French National Police Academy (ENSP).

Cybersecurity threats can broadly be divided into two categories:

- Firstly, **attacks on the functioning of IT systems**. This involves taking control remotely, accessing and disabling systems.
- Secondly, "**information**" **attacks based on identity** theft, defamation and fraud, using false information or exploiting pirated data.

In both cases, the ability of Artificial Intelligence (AI) to automate, to create and to generate content in a variety of forms explains why criminal groups are already experimenting with the use of AI in cyberattacks, confirming the rule that criminals are early adopters of new technologies, which can allow them to increase their profits and scale up their operations.

The hunt for data

To function effectively, AI needs data, as well as the mathematical know-how to design the algorithmic mechanisms to exploit it. The hunt is therefore on to access the information criminals need to feed AI models. For example, the ability of generative AI (LLMs), to produce convincingly realistic content (emails, audio, video, etc.) requires prior knowledge such as the names and functions of the people who are being impersonated, the type of vocabulary they use, etc., as well as the scenarios most likely to lead to the desired actions and outcomes. These may include, for example, sending a fraudulent request purporting to come from a legitimate authority or line manager, or fabricating controversial statements, purportedly by a politician or celebrity, in an attempt to defame or discredit them. In each case, the use of AI makes the fraudulent enterprise more believable by putting in place a mise-en-scène which employs the social codes of its target. Thus, the technology does not create new types of fraud, but it gives them a level of quality and detail that makes them harder to detect.

The threat to data in the context of AI use is not just theft. It also involves data leakage, which can also be unintentional due to a lack of understanding of how the technology works. For example, in the spring of 2023, Samsung Electronics employees entered confidential information belonging to their company into ChatGPT interface[1], potentially making that information accessible to a subsequent user. On its own, a purely technical approach to preventing incidents of this kind (for example, blocking access to LLM sites) is insufficient, since individuals can easily get around such measures by using a personal mobile phone or computer. A more educational approach is therefore needed to limit such misuse.

[1] Samsung Bans Staff's AI Use After Spotting ChatGPT Data Leak, Bloomberg, May 2nd, 2023. https://www.bloomberg.com/news/articles/2023-05-02/samsung-bans-chatgpt-and-other-generative-ai-use-by-staff-after-leak

Click here

How fraud targets human vulnerabilities

The use of deepfakes is perhaps the most striking example of how AI can contribute to frauds which target human vulnerabilities. Thus, at the beginning of 2024, an employee of a Hong Kong company was instructed, during a deepfaked video call with management, to make a bank transfer of 25 million dollars[2]. Everything seemed real, from the appearance of the participants in the meeting, to the vocabulary used to the tone of voice of the protagonists: a perfect illusion that overcame natural reluctance and

procedural rules. The identity fraud was achieved through extensive social engineering and the use of computer vision and image processing tools, combining a long-established fraud technique (impersonating an authority figure within an organisation) with increasingly accessible software capabilities. In addition, the use of interfaces that can be understood by non-specialists means that it is easier to deploy and control these highly complex tools.

[2] *Finance worker pays out $25 million after video call with deepfake 'chief financial officer', CNN, February 4. 2024. https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html*

Click here

Defensive techniques using AI

Mathematical modelling is particularly relevant in a technically standardised world. It works wonders in detecting anomalies, duplications, omissions or superfluous functions in computer programmes. Against a backdrop of a shortage of cybersecurity experts, the use of AI to review software and systems is likely to increase efficiency. This is particularly true for tasks that are tedious and therefore unattractive to practitioners. Algorithms can also be used to establish attack scenarios for training purposes: simulation capabilities that can be used to design protection systems.

While many publishers of AI solutions state in their conditions of use that their tools cannot be used for malicious or fraudulent purposes, the imagination of hackers in formulating production instructions (prompts) enables them to circumvent these technical restrictions.

This exploitation and knowledge of the offensive capabilities of AI is useful for identifying and documenting methods for detecting such actions. Thus, understanding the modus operandi of attackers can be used to develop strategies for identifying and neutralising malware and other fraud vectors, designed or driven by algorithms. The combination of appropriate computing power and human ingenuity to create situations that convince adversaries to carry out certain actions is a particularly effective technique. This type of work is of great interest to military staffs, intelligence services and criminal organisations alike.

Private companies, government departments, local authorities and even private individuals, can all be used as entry points to reach institutional targets and are likely to be targeted by campaigns combining AI technologies and social engineering. More than ever, the boundaries between the military, the business world and the general public are becoming porous, as documented and analysed in the book "frontiers.com"[3].

[3] *Frontières.com, Nicolas Arpagian, Editions de l'Observatoire, 2022.*

AI technologies deployed in the arsenals of governments and their subcontractors

Military parades are a chance for governments to show off the world their military hardware and firepower. It is difficult to transpose this highly symbolic display to cyber resources, even if cybercombat units are increasingly taking their place in such parades, alongside conventional weaponry.

Nevertheless, variations of Artificial Intelligence are already being integrated into the offensive arsenal of governments. In February 2024, for example, Microsoft and OpenAI stated in a security blog[4] that entities affiliated to North Korea, Iran, China and Russia were conducting experiments combining AI and large language models (LLMs) to complete their cyberattack operations. The two companies stated that this involved various phases of the attack chain, such as reconnaissance, coding assistance and malware development. They established that hackers used OpenAI to query open-source databases, perform translations, spot coding errors and perform basic coding tasks. The blog post further states that Microsoft and OpenAI have moved to stop such activities, notably by disabling user accounts associated with certain threat actors assessed to be associated with state agencies.

[4] Staying ahead of threat actors in the age of AI - Microsoft Threat Intelligence – February 14, 2024 - https://www.microsoft.com/en-us/security/blog/2024/02/14/staying-ahead-of-threat-actors-in-the-age-of-ai/

Click here

A legal framework that seeks to anticipate abuses, without restricting innovation

As the ChatGPT wave flooded the world, giving the general public access to its services in November 2022, the governments of the major powers immediately sought to curb the threats arising from the hostile or criminal use of these algorithmic models. In October 2023, President Biden signed an executive order[5] which requires that developers of the most powerful AI systems share their safety test results and other critical information with the US government. This obligation demonstrates how important the US government considers it is to have intimate knowledge of how these complex systems work. China, for its part, has passed a dedicated law[6], which came into force on 15 August 2023. In Europe, in March 2024, the European Parliament approved the final text of a new EU Regulation: the AI Act[7]. The stated aims of the Regulation include “ensuring a high level of protection of health, safety, fundamental rights” against “the harmful

effects of AI systems", while also supporting innovation. The terms used characterise a wish to seek a balance between a desire not to curb innovations that could contribute to the Old Continent's competitiveness and technological leadership, and to leave possible harmful uses, which are still far from being fully documented, unchecked and unregulated.

[5] *Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence - White House - October 30.2023 - https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/* Click here

[6] *Interim Measures for the Management of Generative Artificial Intelligence Services - July 13. 2023 - Cyberspace Administration of China - www.cac.gov.cn/2023-07/13/c_1690898327029107.htm* Click here

[7] *Artificial intelligence act: Council and Parliament strike a deal on the first rules for AI in the world – February 2nd. 2024 - https://www.consilium.europa.eu/fr/press/press-releases/2023/12/09/artificial-intelligence-act-council-and-parliament-strike-a-deal-on-the-first-worldwide-rules-for-ai/* Click here

Conclusion

With the advent of the AI era, governments find themselves subject to challenges to their ability to organise the rules which apply to their societies, and competition to maintain their authority over their populations, and their role in geopolitics. Firstly, states face a challenge to acquire and control the technical infrastructures (GPUs, servers, cloud services, etc.) needed to run Artificial Intelligence models, secondly, to attract and retain the talent capable of designing and driving these arrays of algorithms. And finally, to organise themselves in such a way as to avoid competition from private organisations – whether strictly commercial or criminal – whose size, scope of action and financial clout could challenge the legitimate authority of government bodies.

The speed with which these digital tools can be designed, implemented and disseminated is unprecedented. In addition, their impact extends across the entire spectrum of human activity: health, education, industry, management, the arts, commerce, government, as well as illegal activities. These technological breakthroughs thus require both democratic authorities and citizens to take greater ownership of the issues surrounding Artificial Intelligence.

Contributors

- **Richard Absalom**, *Principal Research Analyst,* **Information Security Forum Limited (ISF)**
- **Nicolas Arpagian**, *Vice President*, **HeadMind Partners**
- **France Charruyer**, *Founder, Lawyer & Partner, IP, IT & Data*, **Altij**
- **Nicholas Cullen**, *Lawyer, Partner, Data, IT & Corporate , Solicitor of England and Wales,* **Altij**
- **Mahé Dersoir**, *Policy Officer at the Cyber Policy Unit,* **Ministère de l'Europe et des affaires étrangères**
- **David Mudd**, *Global Head of Digital Trust Assurance,* **British Standard Institution (BSI)**
- **James Pearn**, *Head of Innovation, Health and Creative - Trade,* **British Embassy Paris**

Chaired by

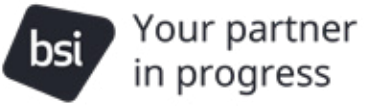
Olivier Campenon, *Chairman of the* **Cross-Channel Institute**, *CEO,* **Group Lefebvre**

Director of publication

Catherine Le Yaouanc, *General Manager,* **Franco-British Chamber**

Coordination

Jérôme Testut *Head of Communications, Marketing & Partnerships,* **Franco-British Chamber**



With the support of

The Cyber Sectoral Analysis is a publication of the Cross-Channel Institute, the think tank of the Franco-British Chamber.

The contributors for this edition are Altij, the British Standard Institution (BSI), HeadMind Partners and the Information Security Forum (ISF). The views and interpretations in this report are exclusively and solely those of the Franco-British Chamber and the aforementioned partners.

Cross-Channel Institute
c/o Franco-British Chamber
22 rue de Londres - 75009 Paris
+33 (0) 1 53 30 81 30
contact@crosschannelinstitute.com
www.crosschannelinstitute.com

Linkedin : Cross-Channel Institute
Twitter : @CrossCInstitute
Instagram : crosschannelinstitute
Facebook : Cross-Channel Institute